Så cybersäkrar du din verksamhet 2026

En digital guidebok fylld med praktiska tips och råd för små och medelstora teknikbolag, anpassad för både medarbetare och ledning.

Funded by the European Union

Initiativtagare:

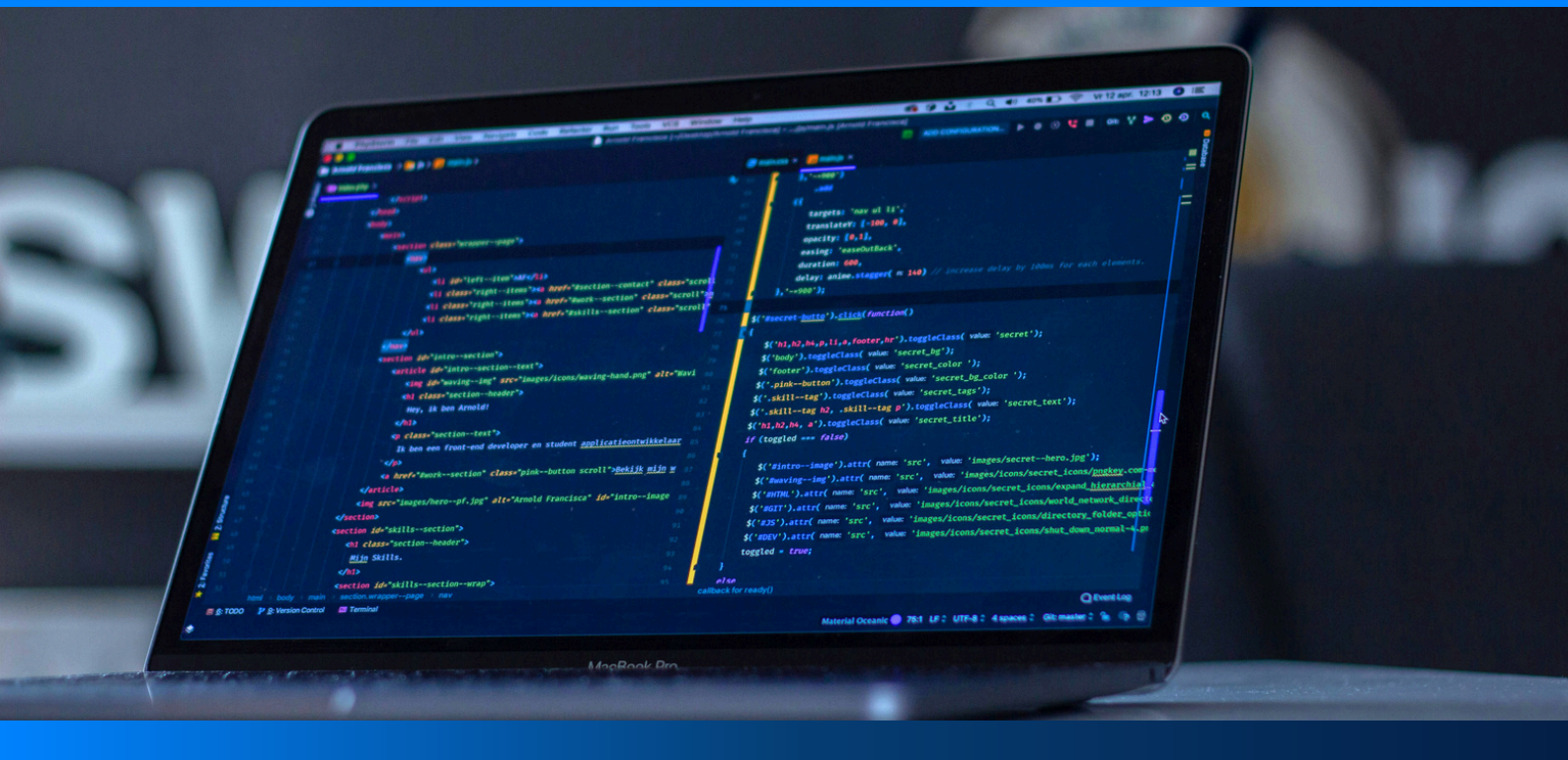
Sweden Secure Tech Hub

SSF

CYBERCAMPUS SVERIGE

Medverkande partner

BOSCH



Innehållsförteckning

Bakgrund

Cybersäkerhet har blivit en avgörande fråga för små och medelstora företag. Cyberattacker blir allt vanligare, och alla typer av företag är utsatta. Samtidigt upplever många att det är svårt att veta var man ska börja, vilken kunskap som krävs och vilket stöd som finns.

Den här guideboken har tagits fram för att sänka tröskeln. De tre nationella aktörerna Sweden Secure Tech Hub, Stöldskyddsföreningen och Cybercampus Sverige har gemensamt tagit initiativ till att göra cybersäkerhet mer tillgänglig och konkret för svenska företag.Tillsammans representerar de forskning, kompetensutveckling och praktiskt säkerhetsarbete – en bred och stabil grund att stå på.

Målet är att erbjuda ett tydligt första steg. I guiden finns konkreta råd, expertperspektiv och vägledning som hjälper företag att komma vidare i sitt säkerhetsarbete. Innehållet är utformat för att vara lätt att ta till sig och möjligt att omsätta i praktiken, oavsett var ni befinner er i dag.

Initiativet drivs av Sweden Secure Tech Hub, Stöldskyddsföreningen och Cybercampus Sverige. Medverkande partner Bosch. Genom sina respektive erfarenheter och expertis inom cybersäkerhet har de tillsammans skapat ett innehåll som är både relevant och användbart.

När kunskap delas och aktörer samarbetar stärks förutsättningarna för verklig förändring. Förhoppningen är att denna guide ska inspirera fler företag att ta nästa steg – och därigenom bidra till ett tryggare och mer motståndskraftigt svenskt näringsliv.

Sweden Secure Tech Hub

Sweden Secure Tech Hub är ett nationellt innovationsnav som stärker cybersäkerhetsförmågan hos små och medelstora företag i Sverige.

Initiativet drivs i samarbete med Kista Science City, Ideon Science Park, Linköping Science Park, Lindholmen Science Park, Blue Science Park och Luleå Science Park.

Projektet medfinansieras av Europeiska unionen, Region Blekinge, Utveckla Norrbotten och Västra Götalandsregionen.

Genom Sweden Secure Tech Hub får företag tillgång till behovsanalyser, expertrådgivning, testmöjligheter och starka nätverk. Stödet är utformat för att vara praktiskt och anpassat efter företagens behov.

Målet är att göra cybersäkerhet till en naturlig del av utvecklingen av produkter och tjänster. Genom att kombinera kompetens från forskning, näringsliv och offentlig sektor skapas bättre förutsättningar för innovation, tillväxt och långsiktigt hållbara digitala lösningar.

BOSCH

Bosch är ett globalt teknik- och tjänsteföretag med lång erfarenhet av att utveckla lösningar inom bland annat industri, mobilitet och uppkopplade produkter. Företaget arbetar brett med digitalisering och har under många år byggt upp en stark kompetens inom cybersäkerhet.

För små och medelstora teknikbolag innebär det att Bosch kan bidra med både kunskap och praktiskt stöd i hur säkerhet integreras i produkter och system från början. Det handlar till exempel om att identifiera risker i utvecklingsfasen, bygga in säkerhetsfunktioner i designen och säkerställa att lösningar uppfyller relevanta krav och standarder.

Genom sin erfarenhet av komplexa system och internationella marknader kan Bosch också ge vägledning kring hur företag kan arbeta strukturerat med cybersäkerhet över tid. För målgruppen blir det ett sätt att minska sårbarheter, stärka förtroendet hos kunder och skapa mer robusta och konkurrenskraftiga produkter.

BOSCH

Fyra steg att cybersäkra din verksamhet

Tips och expertis

Sweden Secure Tech Hub, i samverkan med Bosch

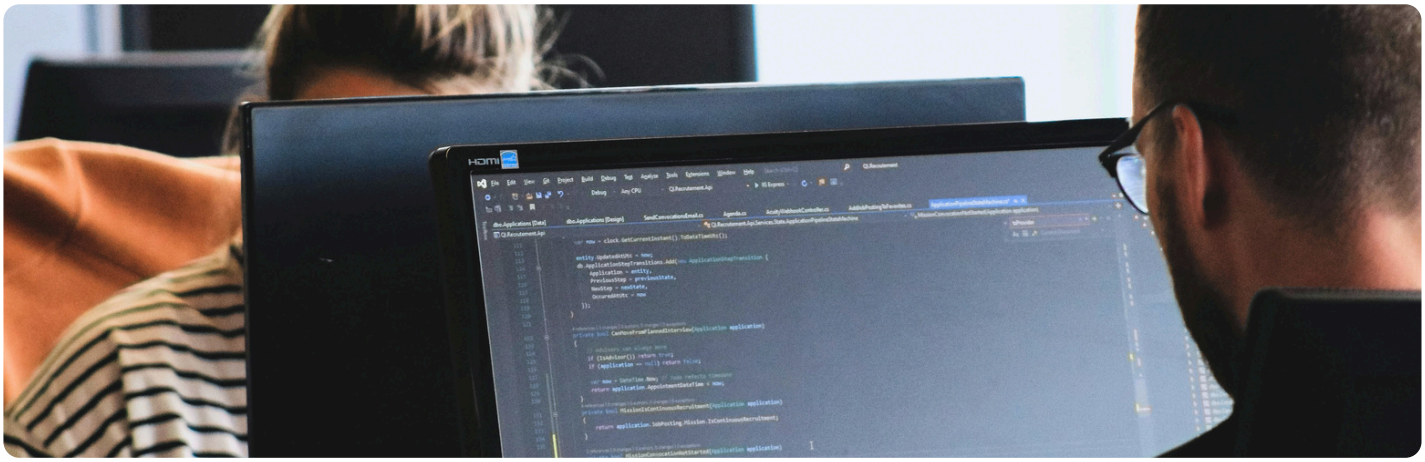
01 Integrera säkerhet tidigt i utvecklingsprocessen (Security by Design)

a. Skifta vänster (Shift Left): Tänk på säkerhet från start. Det är betydligt billigare och effektivare att åtgärda sårbarheter i design- och kodningsfasen än när produkten redan är ute på marknaden.

b. Hotmodellering (Threat Modeling): Redan i designstadiet, analysera potentiella hot och sårbarheter för produkten. Identifiera vilka attacker som är möjliga och vilka konsekvenser de kan få. Detta hjälper er att designa in säkerhetskontroller från början.

c. Säkra kodningsstandarder: Utbilda era utvecklare i säkra kodningsmetoder och standarder. Se till att säkerhetskrav är en del av specifikationerna för nya funktioner.

d. Spårbarhet. Se till att ha spårbarhet från kravmassa hela vägen till testfall och incidenthantering. Detta hjälper er att lösa sent uppkomna brister.



02 Inför robusta test- och granskningsrutiner för era produkter.

a. Automatiserade säkerhetstester: Använd verktyg för tex statisk kodanalys i er CI/CD-pipeline

b. Penetrationstester (Pentests): Låt externa, oberoende cybersäkerhetsföretag utföra penetrationstester på era produkter. De simulerar attacker från verkliga hackare för att hitta sårbarheter som era interna tester kanske missar. Detta är särskilt viktigt före lansering och vid större uppdateringar.

c. Säkra kodningsstandarder: Utbilda era utvecklare i säkra kodningsmetoder och standarder. Se till att säkerhetskrav är en del av specifikationerna för nya funktioner.

Magnus Alinder, Bosch
Head of Cybersecurity Management and Software Security Engineering

03 Hantera sårbarheter och uppdateringar proaktivt under produktens hela livscykel

a. Sårbarhetshantering (Vulnerability Management): Upprätta en process för att ta emot, validera och åtgärda säkerhetsbrister som upptäcks i era produkter, oavsett om de hittas internt eller rapporteras av kunder.

b. SBOM (Software Bill of Materials): Om ni använder tredjepartsbibliotek och komponenter, se till att ni har en SBOM. Den listar alla komponenter och deras versioner, vilket underlättar spårning av sårbarheter som upptäcks i dessa komponenter.

c. Mekanismer för säkra uppdateringar: Se till att era produkter har en robust och säker mekanism för att distribuera säkerhetsuppdateringar till produkterna.

04 Tydliga processer för incidenthantering

a. Incident Response Plan för produkter: Ha en plan för hur ni agerar om en kritisk sårbarhet upptäcks i en produkt som redan är ute på marknaden.

Vem är ansvarig? Hur åtgärdas det? Hur snabbt ska det gå?

Varför ska du söka stöd via Sweden Secure Tech Hub

Vi har intervjuat representanter från Innotech Sverige, InnoviGuard och FixedIT Consulting för att ta del av deras perspektiv.

Vilket stöd får ni av Sweden Secure Tech Hub?

Innotech Sverige: SSTH har erbjudit oss expertrådgivning och stöd i vår behovsanalys. Vi har dessutom fått hjälp med testning och validering av vår produkt, särskilt när det gäller cybersäkerhetsaspekter.

Vilka utmaningar hade ni?

FixedIT Consulting: Stora kunder vill se bevis på IT-säkerhet, ofta via certifieringar som ISO27001 och SOC2. För startups är dessa ofta för dyra och tidskrävande, men enklare dokumentation som white papers, gap-analyser eller penetrationstester räcker ofta.

Hur tror ni att stödet från SSTH kommer hjälpa er i er utveckling som företag?

Innotech Sverige: Främst har vi höga förhoppningar på den cybersäkerhetsrapport från Orange Cyberdefense, som SSTH hjälpte oss att komma i kontakt med. Resultatet kommer att vara mycket värdefullt för oss i framtiden, både vid kundmöten och i samband med eventuella certifieringar som ISO 27001.

Varför ska andra söka stöd?

InnoviGuard: För oss var det en smidig möjlighet få en ISO 27001 liknande genomgång och ge oss en trovärdighet som leverantör till våra kunder.

Innotech Sverige: Stödet ger en fantastisk möjlighet för ett växande företag att kostnadsfritt ta ett stort kliv framåt i sin utveckling.

Stöldsyddsföreningen

Genom att erbjuda relevant och kostnadsfri information, praktiskt stöd och verktyg inom området cybersäkerhet hjälper vi små- och medelstora företag att stärka sin cybersäkerhet. Som en del av vårt arbete erbjuder vi plattformen säkerhetskollen.se i syfte att ge vägledning och verktyg för ökad säkerhet, förebygga risker och stå starkare i en digital verklighet.

Vi genomför även webbinarier med aktuell kunskap och insikter. Via vår hemsida stöldskyddsföreningen.se erbjuder vi ett praktiskt cybersäkerhetsprogram i 6 steg, utformat för att ge en tydlig struktur och stöd för att ta näste steg mot en tryggare och mer motståndskraftig verksamhet.

En norm för grundläggande cyberhygien

Verksamheter som har koll på sin cybersäkerhet skyddar inte bara den egna verksamheten, de skapar också affärsfördelar. Samtidigt bidrar de till ökad trygghet för både kunder och leverantörer. Alla verksamheter bör därför uppnå en grundläggande cyberhygien.

På stoldskyddsforeningen.se kan du ladda ner vår kostnadsfria cybersäkerhetsnorm som innehåller konkreta kontroller för att hjälpa verksamheter i alla storlekar att säkerställa att de uppfyller grundläggande krav på cybersäkerhet.

Ett självtest som hjälper dig att komma i gång

Det kan vara svårt att veta hur du bör prioritera och vilka åtgärder som ger största möjliga effekt med minsta möjliga insats. På säkerhetskollen.se hittar du ett enkelt test som hjälper dig att ”ta tempen” på verksamheten. Du får direkt en överblick över vilka åtgärder som bör prioriteras.

Löpande nyheter som håller dig uppdaterad

Vissa hot är ständigt aktuella, medan andra är akuta för stunden. Säkerhetskollen.se hjälper dig att hålla örat mot rälsen. Där hittar du nyheter som både varnar för pågående attacker och tipsar om nya åtgärder som hjälper dig att stärka verksamhetens cybersäkerhet.

Guider som visar hur du och dina kollegor stärker cybersäkerheten

Många åtgärder är inte alls så krångliga som de låter. På säkerhetskollen.se finns guide som förklarar hur och varför du bör vidta enkla åtgärder som får stor effekt på ditt verksamhets cybersäkerhet. Guiderna riktar sig till både IT-personal och övriga medarbetare.

Webbinarier som gör dig cybersäkrare

SSF genomför också ett antal webbinarier som annonseras på stoldskyddsforeningen.se.

Webbinarierna handlar exempelvis om ledningens ansvar och affärskonsekvenser, att komma i gång utan egen cybersäkerhetsexpert samt struktur och verktyg för vägen framåt.

Vi erbjuder även ett praktiskt cybersäkerhetsprogram i 6 steg, genom stoldskyddsforeningen.se

01 Kom i gång med strukturerat cybersäkerhetsarbete

Stärk din förmåga i hur du prioriterar rätt åtgärder, fördelar ansvar och skapar uppföljning i ditt cybersäkerhetsarbete. Målet är att ge dig en tydlig struktur som stärker både säkerheten och affären.

02 Praktisk tillämpning av SSF-normen Cybersäkerhet Bas

Vi ger dig konkret stöd i hur du omsätter kraven i normen SSF Cybersäkerhet Bas (SSF 1101) till praktiska åtgärder i din verksamhet. Du inleder med en nulägesanalys som visar var ni står och vad ni behöver prioritera.

03 När något händer: Agera rätt

Utveckla din kompetens inom incidenthantering, dataintrång och störningar i verksamheten. Fokus ligger på kontinuitet, ansvar och hur du förbereder dig genom enkla och effektiva övningar.

04 Medarbetare, en viktig resurs

Tekniken är en del av säkerhetsarbetet och människan är en annan. Förbättra din kapacitet i hur du gör din personal till en aktiv del av cybersäkerhetsarbetet och bygger beteenden som håller över tid.

05 Säker AI-användning i verksamheten

AI används redan i många verksamheter men ofta utan styrning. Här stärker du din förmåga att dentifiera risker, sätta ramar och använda AI på ett säkert och kontrollerat sätt.

06 Leverantörskrav och affärsvärde

Levererar du till en verksamhet eller kommun som omfattas av cybersäkerhetslagen?
Här får du insikter om hur cybersäkerhet kan bli en affärsfördel genom minskad risk och ökad tillit, till exempel genom certifiering.

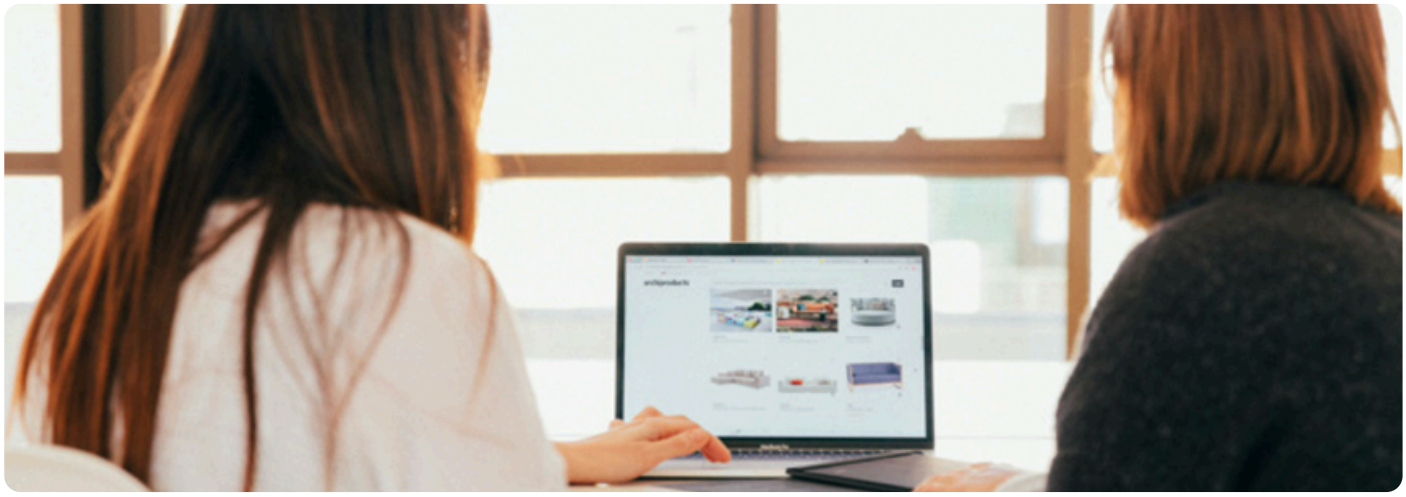
> “Cybersäkerhet är inte en kostnad utan en affärsfördel. Certifiering visar att ni tar säkerhet på allvar.“

CYBERCAMPUS SVERIGE

Cybercampus Sverige är ett svenskt nationellt initiativ och samarbete mellan universitet, forskningsinstitut, myndigheter och företag.

Cybercampus möjliggör utbildning, forskning och innovation inom cybersäkerhet och cyberförsvar utöver vad som är möjligt för ett enskilt universitet, institut, myndighet eller företag. Syftet är att öka landets cybersäkerhet, att stärka samhällets försvarsförmåga och svensk konkurrenskraft.
Bland Cybercampus partners och medlemmar finns företag, myndigheter, forskningsinstitut och lärosäten.

Små och medelstora företag är en huvudmålgrupp för Cybercampus. Eftersom 97 % av landets företag har färre än tio anställda är det otroligt viktigt att det finns bra och anpassade möjligheter för kompetensutveckling. Nya hot och behov kräver konstant uppdatering av kompetenser.



Guide för kompetensutveckling i cybersäkerhet

Med rätt kunskap i cybersäkerhet blir det lättare att upptäcka risker i tid, förebygga incidenter och skydda både företaget och era kunder. Det behöver inte vara krångligt – men det kräver att ni satsar på rätt kompetensutveckling. Cybercampus Sverige har tagit fram en guide för detta.

När ni investerar i cybersäkerhetskunskap visar ni också att ni tar säkerhet på allvar. Det stärker förtroendet hos kunder, samarbetspartners och leverantörer.

01 Definiera era behov

Börja med att ta reda på vad just ert företag behöver. Alla företag har olika risker och olika förutsättningar. Därför är det viktigt att inte börja med utbildning direkt, utan först förstå var kunskapsluckorna finns.

På Cybercampus.se finns en ifyllbar mall som hjälper er att identifiera områden där ni är sårbara. Svaren hjälper er att se vilken kunskap ni behöver.

Om ni vill identifiera vilka specialistroller som kan behövas, kan ni ta hjälp av EU-organet Enisas kompetensprofiler.

02 Sätt rätt nivå och ha realistiska förväntningar

Alla i företaget behöver inte bli experter på cybersäkerhet. Det viktiga är att rätt personer har rätt kunskap för sina uppgifter.

Fundera på vilken nivå som är rimlig. Vad behöver ledningen, och vad behöver alla medarbetare? När behövs mer fördjupad specialistkunskap? Omfattas er organisation direkt eller indirekt av cybersäkerhetslagen? Vid rekrytering är det viktigt att kraven i annonser och kompetensprofiler är realistiska. För höga eller otydliga krav kan göra det svårt att hitta rätt person.

Kompetensutveckling tar tid. Förvänta er inte omedelbara resultat, utan räkna med att riskerna minskar steg för steg.

03 Skapa rätt förutsättningar i företaget

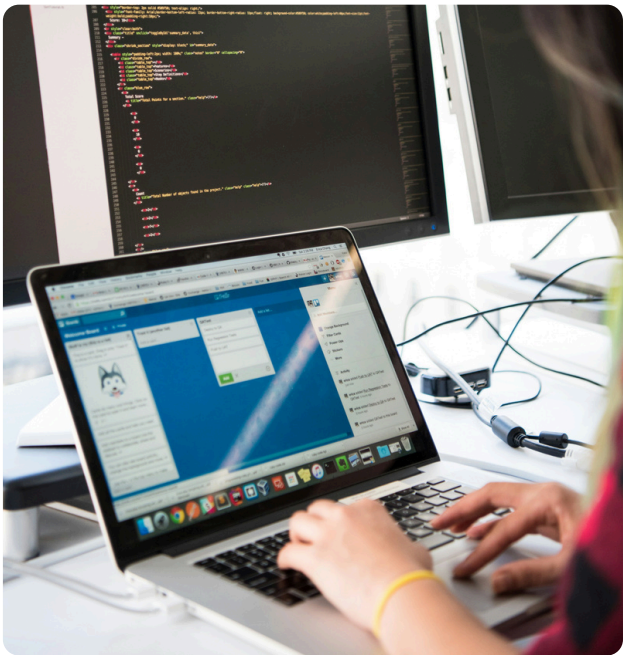
Kompetensutveckling behöver prioriteras för att bli av. Ansvaret ska inte ligga på medarbetaren – bestäm i stället vem som ska gå vilken utbildning, när den ska ske samt hur mycket tid och pengar som kan avsättas. Börja med de personer och områden där behoven är störst.

04 Matcha kompetensgap och rätt åtgärder

Välj utbildningsinsats som möter de kompetensbehov ni har identifierat. Ta reda på vilken utbildning som finns tillgänglig och hur mycket tid den kräver, så att den går att kombinera med er dagliga verksamhet. Ni kan ta hjälp av enkla tester eller behovsbedöm

05 Satsa på kontinuerlig utbildning

Cybersäkerhet är inget engångsprojekt. Hoten förändras, tekniken utvecklas och nya arbetssätt införs. Därför behöver kunskaperna uppdateras löpande. Gör kompetensutveckling till en naturlig del av verksamheten, gärna med en enkel utbildningsplan som följs upp regelbundet. Aktuell och relevant kunskap minskar risken för incidenter – och stärker samtidigt företagets konkurrenskraft.



06 Följ upp och se vad ni har uppnått

Det är viktigt att ta reda på vad genomförda utbildningsinsatser faktiskt har lett till. Har förståelsen ökat, har arbetssätten förändrats, har medarbetarna lättare att hantera risker i vardagen? Den här uppföljningen blir enklare om ni satt upp tydliga mål från början.

”Många svenska företag befinner sig i dag i ett tidigt skede när det gäller strukturerat cybersäkerhetsarbete. Mognadsbedömningar visar att det ofta saknas tydliga roller, uppföljning och helhetsgrepp, samtidigt som allt fler företag berörs – direkt eller indirekt – av nya EU-regelverk som NIS2 och CRA.

Det handlar oftast inte om bristande vilja, utan snarare om att man inte alltid har full insyn i sitt eget nuläge, ansvar eller vilka krav som faktiskt gäller. Om cybersäkerhet inte är integrerad i affärs- och produktutveckling kan det uppstå gap mellan de risker företaget exponeras för och den organisatoriska beredskapen. Det ökar risken för exempelvis phishing eller ransomware-attacker, och kan leda till förlorad data, förtroendeförlust och ekonomiska bortfall.

När det gäller kompetensutveckling krävs det inte alltid stora eller drastiska insatser. För vissa företag kan expertkompetens vara nödvändig, men för många är det viktigaste att successivt höja den grundläggande kunskapen hos hela organisationen. I Sverige finns ett gott utbud av verksamhetsnära utbildningar.”

Mette Svensson,
Affärsutvecklare inom utbildning,
Cybercampus Sverige

Sweden Secure Tech Hub

Första steget till cybersäker verksamhet

Är du ett företag och vill ta er cybersäkerhet till nästa nivå? Vi guidar er till rätt stöd för att driva ert företag framåt och stärka er säkerhet.

Sweden Secure Tech Hub är ett nationellt innovationsnav som stärker små och medelstora företags kapacitet inom cybersäkerhet. Vi vill hjälpa ditt företag att växa tryggt och nå nya höjder. Ansök om stöd hos oss redan idag!

Sök stöd via vår hemsida:

swedensecuretechhub.se

Typ av stöd vi erbjuder:

01	Behovsanalys	Vårt digitala snabbtest ger en överblick och identifierar utvecklingsmöjligheter. Vi tittar även på dina leverantörskedjor för att stärka säkerheten och identifiera förbättringsområden.
02	Expertrådgivning	Få skräddarsydd vägledning för att stärka både produkt- och organisationssäkerhet, med insikter anpassade efter er bransch. Vi hjälper er även med att hitta finansiering för vidare åtgärder.
03	Test och validering	Vi testar och validerar era system i realtid, minska risker och stärker säkerheten med specialiserad träning, hot-simuleringar och certifieringsstöd.
04	Nätverk	Vi stödjer er i att bygga starka nätverk inom cybersäkerhetsekosystemet genom att kartlägga viktiga aktörer och underlätta riktad matchmaking med relevanta partners för er.

Co-funded by the European Union

IDEON SCIENCE PARK

LINKÖPING SCIENCE PARK

Swedish Agency for Economic and Regional Growth

BLUE SCIENCE PARK

SCIENCE PARK

Lindholmen Science Park

Kista Science City

REGION BLEKINGE

UTVECKLA NORRBOTTEN

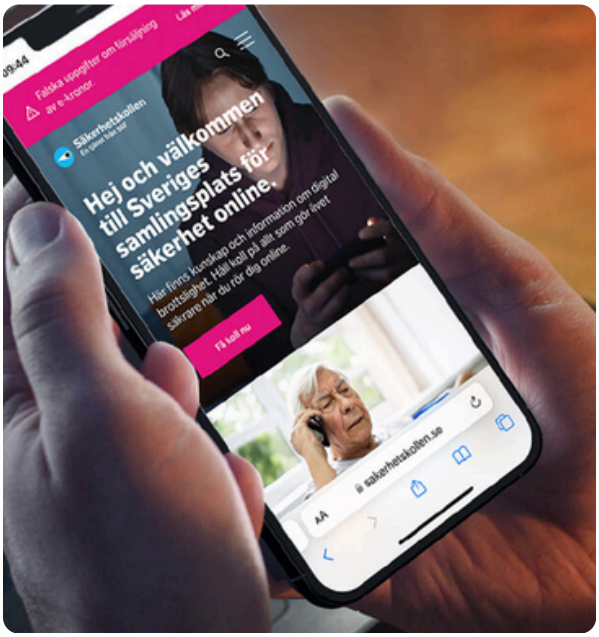
VÄSTRA GÖTALANDSREGIONEN

SSF roll i cybersäkerhetsarbetet

SVi är utpekade i regeringens nationella cybersäkerhetsstrategi och en viktigt pusselbit i samhällets samlade cybersäkerhetsarbete. Tillsammans med Polisen och Nationellt Cybersäkerhetscentrum (NCSC) har vi ett uppdrag att utveckla stödet inom cybersäkerhet och minska antalet cyberbrott hos små och medelstora verksamhet. Arbetet drivs framför allt genom att erbjuda kostnadsfri information, rådgivning och tester på SSF:s plattform säkerhetskollen.se. Plattformen riktar sig till både IT personal och övriga anställda.

SSF erbjuder också verksamhetsanpassade utbildningar inom cybersäkerhet via stoldskyddsforeningen.se, som förstärker och kompletterar det kostnadsfria stödet på säkerhetskollen.se.

SSF är en ideell och oberoende organisation som arbetar brottsförebyggande till stöd för allmänhet och privatpersoner. Det gör vi genom kostnadsfri rådgivning, framtagande av säkerhetsnormer och utbildning.



Typ av stöd vi erbjuder:

01

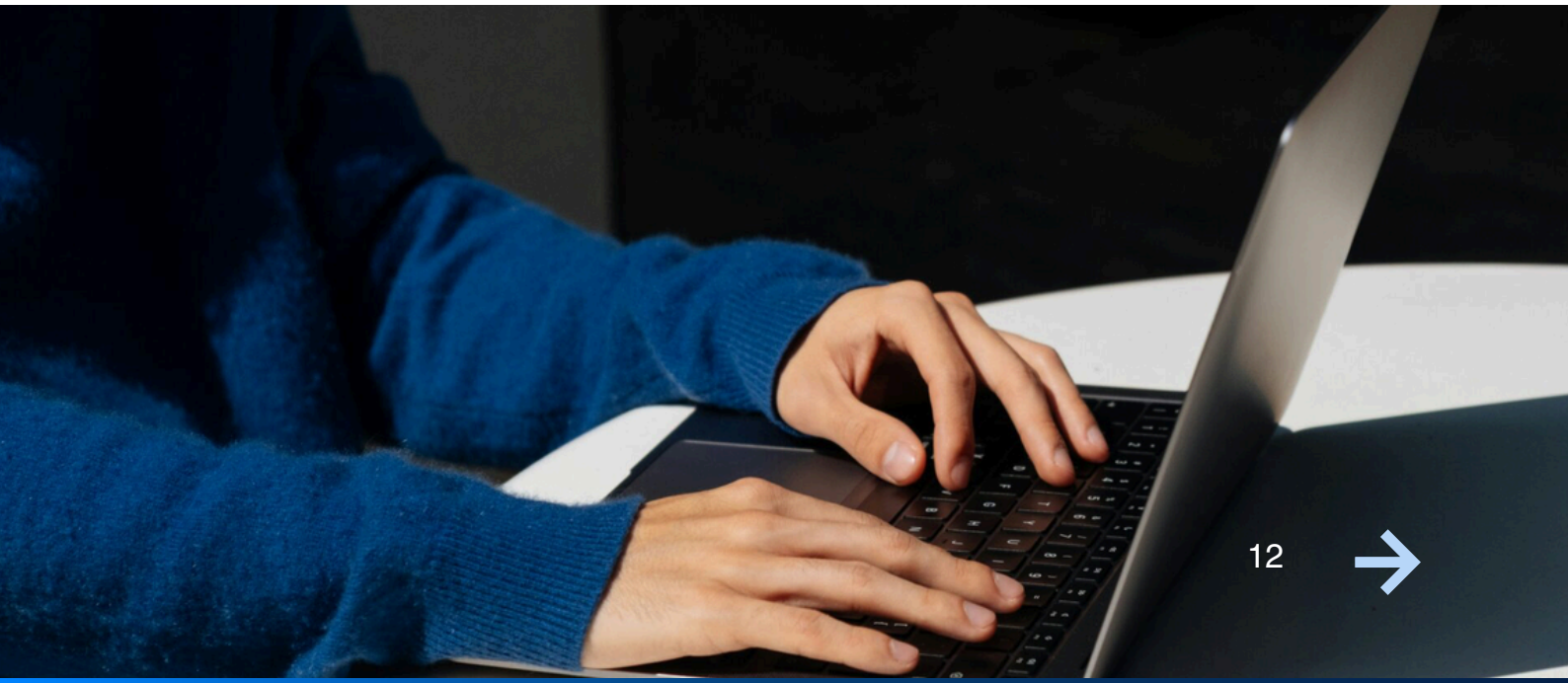
Gå in på säkerhetskollen.se och testa din cybersäkerhet samt ta del av guider och information.

02

Läs mer om våra verksamhetsanpassade cybersäkerhetsutbildningar på stoldskyddsforeningen.se.

03

Anmäl dig till våra webbinarier via stoldskyddsforeningen.se och stärk din cybersäkerhet.



CYBERCAMPUS SVERIGE

Cybercampus arbetar inom utbildning, forskning och innovation. Inom utbildning ska Cybercampus vara med och forma och erbjuda utbildning som möter olika branschers och sektorers kompetensbehov.

Det saknas i dag en samlad bild av kompetensbehovet inom cybersäkerhet i Sverige. Cybercampus möter, som enda nationella samlande aktör, denna utmaning genom att fungera som ett nav, en första ingångspunkt för att hitta relevant cybersäkerhetsutbildning för yrkesverksamma.

Arbetet med utbildningar för yrkesverksamma sker i samverkan mellan Cybercampus samarbetspartners inom högre utbildning och knyter samman befintligt utbud runt om i Sverige. Ofta efterfrågas tvärfunktionell kompetens, som innefattar såväl djupt tekniskt kunnande som juridiska aspekter och ledningsfrågor. Yrkeshögskolor och högskolor har många möjligheter att möta kompetensbehoven inom privat och offentlig sektor. I de fall det saknas befintliga utbildningar kan nya skapas.

Arbetet med utbildningar för yrkesverksamma sker i samverkan mellan Cybercampus samarbetspartners inom högre utbildning och knyter samman befintligt utbud runt om i Sverige. Ofta efterfrågas tvärfunktionell kompetens, som innefattar såväl djupt tekniskt kunnande som juridiska aspekter och ledningsfrågor. Yrkeshögskolor och högskolor har många möjligheter att möta kompetensbehoven inom privat och offentlig sektor. I de fall det saknas befintliga utbildningar kan nya skapas.

Ungefär 80 % av alla svenska företag efterfrågar riktad utbildning och verksamhetsnära stöd, men färre än 20 % utbildar sin personal i cybersäkerhet. Via partnerorganisationerna KTH, Linköpings universitet och RISE har Cybercampus vänt sig till Cybernodens medlemsföretag för att ta reda på vilka ämnesområden som är viktigast samt vilka utbildningsformat som föredras – för att på så sätt kunna erbjuda och utveckla utbildningar som passar svenska företags behov.

Typ av stöd vi erbjuder:

01

Hjälp att identifiera vilken kunskap och kompetens just er verksamhet behöver.

02

Vi samlar kontinuerligt relevanta kurser inom cybersäkerhetsområdet från ledande lärosäten samt skapar kurspaket och utvecklar nya kurser.

03

Hjälp att matcha era behov och er mognadsnivå med rätt utbildningsinsats - om det behövs utvecklar vi helt nya utbildningsinsatser.

Kontakt:

Mette Svensson, affärsutvecklare utbildning
mette@cybercampus.se
+46 737 652 341

Så cybersäkrar du din verksamhet 2026 är en praktisk och lättillgänglig guide fylld med konkreta tips, råd och insikter från experter inom cybersäkerhet.

Boken är framtagen för att stötta små och medelstora teknikbolag i arbetet med att stärka sin digitala säkerhet. Den ger vägledning i hur risker kan identifieras, hanteras och förebyggas – samt hur ett långsiktigt och hållbart skydd kan byggas upp.

Initiativet drivs av Sweden Secure Tech Hub, Stöldskyddsföreningen och Cybercampus Sverige. Medverkande partner Bosch. Genom sina respektive erfarenheter och expertis inom cybersäkerhet har de tillsammans skapat ett innehåll som är både relevant och användbart.Tillsammans bidrar de med bred erfarenhet från forskning, utbildning och praktiskt säkerhetsarbete.

Innehållet riktar sig till både medarbetare och ledning, och fungerar som ett stöd i det dagliga arbetet med att skapa förståelse, engagemang och konkreta åtgärder i hela organisationen – med målet att stärka den digitala motståndskraften i svenska teknikbolag.

Funded by the European Union

Initiativtagare:

Sweden Secure Tech Hub

SSF

CYBERCAMPUS SVERIGE

Medverkande partner

BOSCH