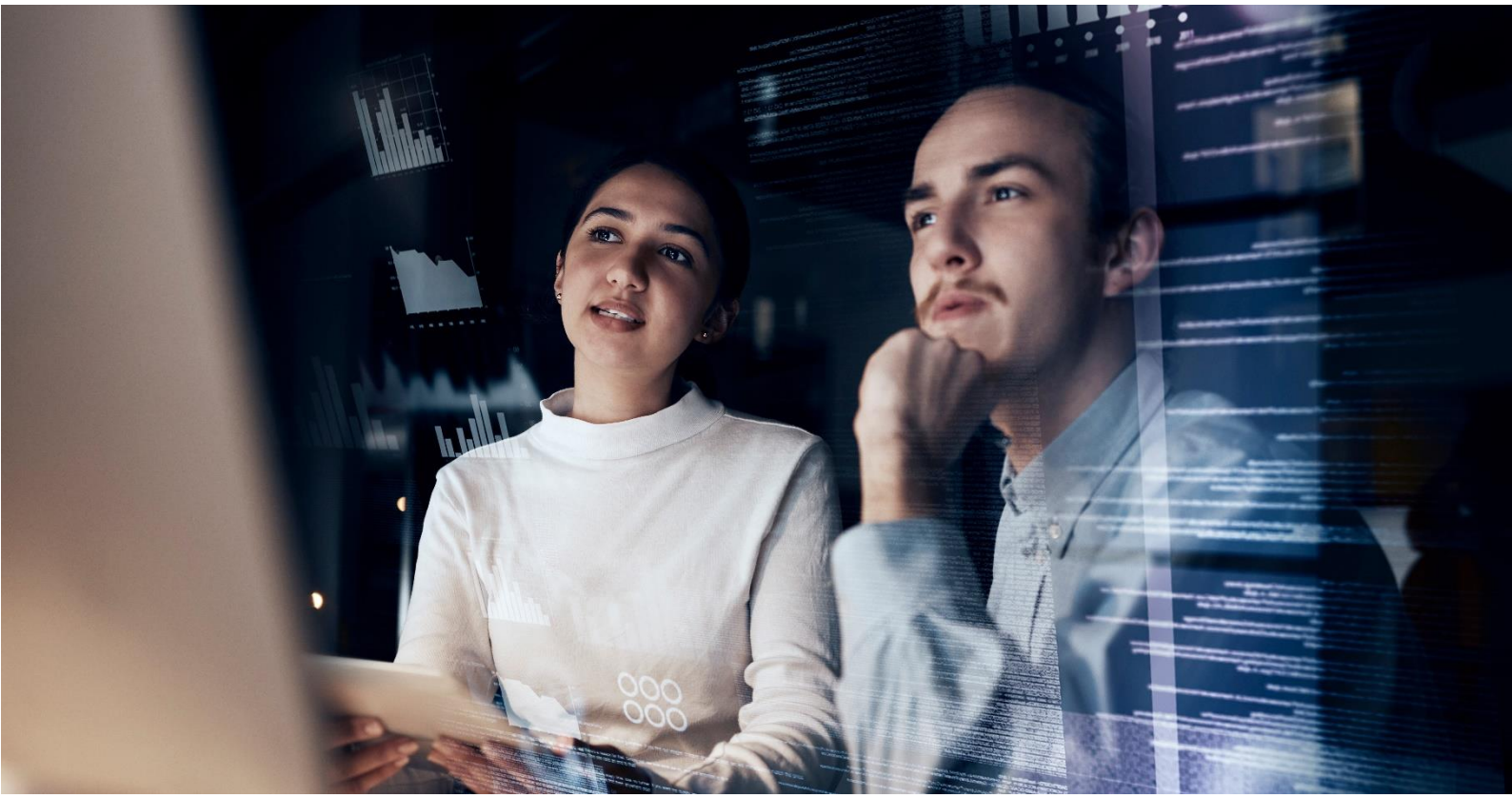
IT-säkerhetsingenjör

Utbildningsplan



Utbildningens namn: IT-säkerhetsingenjör

Ansvarig utbildningssamordnare: Yrkeshögskolan i Enköping, Enköpings kommun

Omfattning, poäng: 400

Studieform: Bunden

Studietakt: Heltid

Examensbeteckning: Utbildningen ger yrkeshögskoleexamen

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76

Innehåll

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76

Yrkeshögskolan

Förkunskapskrav

Kurser

Lägst betyget E/3/G i följande kurser eller motsvarande kunskaper:

- Svenska 2 eller Svenska som andraspråk 2
- Engelska 6
- Matematik 2 eller Nätverkssäkerhet eller Nätverksteknik eller Programmering 1

Motivering av förkunskaper kurser

Den studerande behöver ha goda grundläggande språkliga kunskaper för att kunna tillgodogöra sig utbildningen och nå läromålen. Vidare behövs goda språkliga kunskaper på både svenska och engelska för att kunna verka inom IT- och cybersäkerhet i en kontext där dels många hot kommer från en global arena och dels många organisationer har engelska som koncernspråk.

Goda kunskaper i svenska krävs också för en expertroll där komplexa tekniska lösningar ofta behöver kommuniceras till många olika berörda parter. Vidare krävs goda språkliga kunskaper för att förstå, bearbeta och tillämpa juridiska och tekniska texter och dokument.

Därför anser medverkande arbetsliv att Engelska 6 och Svenska 2 är rätt nivå. Motsvarande kunskaper kan ha tillägnats på annat sätt och då säkerställs motsvarande kunskapsnivå genom prov eller validering av reell kompetens.

Den studerande behöver vidare ha grundläggande kunskaper inom något av områdena matematik, programmering eller nätverksteknik. Ett av dessa områden ger tillräckliga förkunskaper för att den studerande ska kunna tillgodogöra sig kurserna och nå kunskapsmålen.

Motsvarande kunskaper kan ha tillägnats på annat sätt och då säkerställs motsvarande kunskapsnivå genom prov eller validering av reell kompetens.

Mål och krav för examen

- YH-programmet bedöms möta en yrkeshögskoleexamen nivå 5 SEQF utifrån den kunskapsfärdighets- och kompetensnivå som krävs för att kunna genomföra specialiserade arbetsuppgifter inom utveckling, förvaltning och drift av IT-säkerhetssystem.
- Den studerande behöver ha kompetens att konfigurera och bygga system och nätverk för IT-säkerhet. Den studerande erhåller specialiserade kunskaper för att förstå, förklara, felsöka, analysera och åtgärda olika typer av problem, hot och situationer kopplade till IT-säkerhet.

- De studerande behöver också kunna kommunicera detta på svenska och engelska med kollegor, specialister, kunder och beställare. För att nå önskad kompetensnivå ger utbildningen utrymme för omfattande teoretiska studier på eftergymnasial nivå, samt löpande praktiska moment för att implementera och förankra kunskaperna i en realistisk kontext.

- Den studerande ska kunna redovisa och implementera sina kunskaper muntligt, skriftligt och praktiskt, samt använda och förstå den för yrkesrollen tillämpade terminologin. Den studerande ska förstå och tillämpa de kvalitetskriterier som krävs för yrkesrollen inom området IT-säkerhet.

Efter avslutad utbildning ska den studerande ha kunskaper om/i:

- Regelverk, ramverk och kvalitetsstandarder som används inom IT-säkerhet, nationellt och på EU-nivå

- Huvuddragen inom ISO (27001, 27002) samt exempelvis CIS och CC

- Säkerhetsfunktioner som är anpassade till rådande IT-miljö under alla faser (utveckling, test och produktionsstadierna) och vad verksamheten ska utföra genom att använda tex. BKS, loggning, back up, övervakning

- Hur man åtgärdar sårbarheter i operativsystem med härdning

- Utmaningarna med att bygga säkra system med hjälp av virtualisering och molnbaserad lagring

- Nätverkssäkerhet och dess användningsområden

- Modeller för nätverkssegmentering (fysisk-logisk separering) och vanliga tekniker och komponenter (brandväggar, trafikfiltrering, IDS, IPS, övervakning)

- Funktion och användning av nätverkskomponenter som routrar och switchar, samt härdning av dessa

- Nätverk och deras användningsområden (topologi)

- Användning och behov av signalskydd/krypto

- Relevanta förvaltningsverktyg för yrkesrollen

Efter avslutad utbildning ska den studerande ha färdigheter i att:

- Genomföra regelverksanalys och tillämpa regelverk (ex. KSF) inom IT-säkerhetsområdet
- Genomföra verksamhetsanalys
- Tillämpa agila IT-utvecklingsmodeller (t.ex. DevOps, Scrum eller Kanban)
- Tillämpa etiska värderingar, hur kan regelverk följas, och samtidigt utföra handlingar som är etiskt försvarbara
- Genomföra sårbarhets-, hot- och riskanalys, identifiera risker och sårbarheter samt tolka och värdera resultatet
- Utifrån resultat av sårbarhetsanalys föreslå lämpliga åtgärder för förbättring eller skydd
- Tillämpa BKS, behörighets- och kontrollsystem, samt tillämpa behörighetsstyrning inom yrkesrollen
- Bygga nätverk och administrera nätverk med fokus på säkerhet
- Montera och konfigurera routrar och switchar
- Tillämpa kryptologi/kryptering vid behov
- Utföra sårbarhetsskanning av system och nätverk med olika typer av verktyg samt beskriva olika testverktygs användningsområden
- Genomföra felsökning i drift
- Använda och anpassa hårdvara utifrån verksamhetens identifierade behov och uppgifter
- Tillämpa principer för automation och fjärrstyrning
- Upprätta brandväggar och lösning för fjärråtkomst , ex. VPN
- Kunna läsa, tolka och skriva programmeringsspråk som förekommer i yrkesrollen
- Kommunicera och resonera kring komplexa problemställningar samt föreslagna åtgärder och lösningar med nationella och internationella branschföreträdare och aktiva inom yrkesområdet.

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76

Yrkeshögskolan

Efter avslutad utbildning ska den studerande ha kompetenser att:

- Utifrån befintlig säkerhetsanalys värdera risker för säkerhetsangrepp
- Utifrån resultat utforma säkerhetsskydd av den egna organisationens system och information
- Använda agila projektmetoder i utveckling, test och driftsfas
- Använda och anpassa datakommunikation utifrån verksamhetens behov och säkerhetsläge
- Självständigt anpassa loggar och larm utifrån identifierade behov och risker för verksamheten
- Använda kryptering och signering i samband med molntjänster
- Analysera behov av trafikskydd och applicera trafikskydd
- Analysera risken för säkerhetshot och skydda den egna organisationens system och information mot dessa hot
- Implementera virusskydd, härdning och loggning i virtuella miljöer
- Upprätta olika typer av säkerhet/skydd utifrån identifierat behov (ex. fysiskt skydd, skalskydd, RÖS, tillträdesrätt, mekaniska lås, elektroniska passersystem, larm, sektionering i byggnad samt bevakning) • Installera, konfigurera, felsöka och härda operativsystem (företrädesvis Windows och Linux).

Terminstider

Höstterminen 2024

Måndag 16 september – fredag 20 december (14 veckor)

Vårterminen 2025

Måndag 13 januari – fredag 20 juni (23 veckor)

Höstterminen 2025

Måndag 11 augusti – fredag 26 december (20 veckor)

Vårterminen 2026

Måndag 12 januari – fredag 19 juni (23 veckor)

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76

Yrkeshögskolan

Kursöversikt

Kursnamn (YH-poäng)

- Branschöversikt och säkerhetsprövning (15)
- Ethical Hacking (30)
- Examensarbete (20)
- Härdning (35)
- Informationssäkerhet (55)
- IT-juridik (20)
- LIA - Lärande i arbete (100)
- Nätverksteknik (50)
- Operationell teknik (10)
- Säker molnstrategi (25)
- Virtualiseringsteknik och automation (40)

Sammanlagt 400 YH-poäng

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76

Yrkeshögskolan

Kurser

Branschöversikt och säkerhetsprövning (15p)

Syfte och mål:

Kursens syfte är att behandla branschstandarder för cyber- och informationssäkerhet. Den går igenom branschen, dess aktörer, yrkesrollen, konsultrollen och närliggande yrkesroller. Kursen behandlar även anonymiserat arbete och säkerhetsprövning.

Kursen ger kunskaper i/om:

- Yrkesrollen
- Konsultrollen och närliggande yrkesroller
- Branschens aktörer, yrkesroller och utveckling
- Anonymiserat arbete
- Säkerhetsprövning
- Efter avslutad kurs ska den studerande ha färdighet att:
- Ge exempel på svenska myndigheter med ett utpekat ansvar på IT-säkerhetsområdet och hur de samverkar
- Ge exempel på lagkrav från civil och militär sektor inom IT-säkerhet
- Förklara hur svenska företag med digitala tjänster påverkas av EU:s NIS direktiv kopplat till åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem

Efter avslutad kurs ska den studerande har kompetens att:

- Föreslå litteratur på området Informationssäkerhet
- Beskriva Informationspåverkan och ge några exempel
- Ge exempel på vanliga IT-angrepp mot en privatperson
- Ge exempel på vanliga IT-angrepp mot ett företag
- Beskriva en enkel metod för Incidentrapportering av IT-angrepp

Ethical hacking (30p)

Syfte och mål:

Kursens syfte är att ge de studerande färdighet i att genomföra säkerhets- och sårbarhetsscanningar av IT-system med både teoretiska analyser och mjukvaruverktyg. Målet är att de studerande ska kunna agera som angripare mot ett utvalt IT-system eller nätverk i syfte att både förstå vad en angripare kan göra och om dess aktiviteter kan upptäckas för att sedan föreslå strategier för att skydda nätverket mot angrepp.

Kursen ger kunskaper i/om:

- Principer för etisk hackning
- Teoretisk analys av sårbarheter i ett IT-system
- Planering och genomförande av sårbarhetsscanning med kommersiella programvaror
- Utvärdering av testresultat och framtagande av säkerhetsåtgärder
- Tillgängliga öppna källor för att inhämta underlag för sårbarheter i programvaror och dator- samt nätverkskomponenter
- Penetrationstestverktyg och dess funktioner

Efter avslutad kurs ska den studerande ha färdighet att:

- Genomföra olika typer av säkerhets- och sårbarhetsscanning av IT-system med både teoretiska analyser och mjukvaruverktyg
- Planera och genomföra sårbarhetsscanning av IT-komponenter och IT-system med kommersiella programvaror
- Upprätta rutiner för att underhålla och utveckla befintliga skydd mot obehörigt intrång samt minimera riskerna för angrepp under ett IT-systems livscykel
- Tolka resultat av sårbarhetsscanning och omsätta dessa i lämpliga skyddsåtgärder
- Utveckla penetrations-testfall och genomföra penetrationstestning enligt testspecifikationer

Efter avslutad kurs ska den studerande har kompetens att:

- Redogöra för tillgängliga öppna källor för att inhämta underlag för sårbarheter i programvaror och dator- samt nätverkskomponenter
- Tolka information från öppna källor om kända sårbarheter i programvaror och dator- samt nätverkskomponenter och hur den applicerar på ett typiskt IT-system
- Tillämpa principer för etisk hackning för att beskriva IT-systemets och nätverkets svagheter

Examensarbete (20p)

Syfte och mål:

Kursens syfte är att den studerande ska fördjupa sina kunskaper, färdigheter och kompetenser inom IT-säkerhet genom att planera, genomföra, analysera och föreslå eller utföra åtgärder för ett egenvalt examensprojekt inom ITsäkerhet eller annan utvald problemställning relevant för ämnesområdet. Målet är att den studerande självständigt ska kunna planera, strukturera, avgränsa, genomföra samt skriftligt och muntligt presentera sitt arbete.

Kursen ger kunskaper i/om:

- Fördjupad kunskap inom ett eller flera områden i kursplanen
- Fördjupad produktionskunskap inom ett egenvalt område
- Fördjupad förståelse för och analys av av ett egenvalt område
- Att strukturera, avgränsa och planera och genomföra ett egenvalt arbete
- Skriftlig, visuell och muntlig presentation av examensarbetet

Efter avslutad kurs ska den studerande ha färdighet att:

- Planera, strukturera, avgränsa och genomföra ett arbete samt att skriftligt och muntligt presentera sitt arbete
- Redogöra för sin samlade kunskap i detektering, analys och förebyggande IT-säkerhetsarbete så att arbetets resultat och slutsatser kan omsättas i praktik
- Visa på färdigheter och kompetenser inom utveckling, förvaltning och drift av IT-säkerhet, IT-system och nätverk
- Tillämpa och kommunicera, nationellt och internationellt, med rätt nomenklatur och terminologi för yrkesrollen
- Söka information och fördjupa sina kunskaper inom yrkesområdet genom att använda aktuella studier, branschlitteratur eller dokumentation, rapporter eller andra dokument

Efter avslutad kurs ska den studerande har kompetens att:

- Planera, strukturera, avgränsa och genomföra ett egenvalt arbete, samt att skriftligt, muntligt och visuellt presentera detta på ett målgruppsanpassat sätt
- Argumentera muntligt inför en grupp om sin valda lösning
- Motivera och argumentera skriftligt och muntligt för vald lösning utifrån IT-säkerhetsperspektiv

Härdning (35p)

Syfte och mål:

Kursens syfte är att ge de studerande färdighet i att föreslå och genomföra olika typer av härdning för operativsystem och nätverkskomponenter. Målet är att den studerande ska kunna applicera härdning och ha kunskap om vilka valmöjligheter som finns för att rätt avväga funktionalitet mot säkerhet.

Kursen ger kunskaper i/om:

- Operativsystemhärdning
- Datorsäkerhet för Linux och Windows
- Härdning av nätverkskomponenter (brandväggar, routrar)
- Härdning av virtuella system
- Virtualiseringsanpassat virusskydd
- Krypteringslösningar för virtuella system
- Skillnaden mellan att härda traditionella datormiljöer och att härda virtuella dator- och nätverksmiljöer
- Best practices för härdning av operativsystem, inbyggda program (firmware), nätverkskomponenter, databaser och andra applikationer.

Efter avslutad kurs ska den studerande ha färdighet att:

- Föreslå och genomföra olika typer av härdning för operativsystem och nätverkskomponenter
- Skilja på att härda traditionella datormiljöer och att härda virtuella dator - och nätverksmiljöer
- Genomföra installation och härdning med fokus på servrar (Windows och Linux)
- Konfigurera IT-system (företrädesvis Windows och Linux)
- Använda active directory (AD) och group policy objects (GPO) för behörighetsstyrning
- Sammanställa konfigurationer för användning i systemdokumentation
- Kunna läsa ut aktuell konfiguration och härdning för ett IT system med kommersiella verktyg
- Tolka script- och kodspråk med hjälp av exempelvis Powershell

Efter avslutad kurs ska den studerande har kompetens att:

- Applicera härdning utifrån de valmöjligheter som finns för att rätt avväga funktionalitet mot säkerhet.

Informationssäkerhet (55p)

Syfte och mål:

Kursens syfte är att ge de studerande kunskaper om informationssäkerhet i IT-system och åtgärder för att förbättra och utveckla dessa samt förebygga dataintrång. Målet är att de studerande ska uppnå specialiserad kunskap om hur information i IT-system kan skyddas med avseende på sekretess, tillgänglighet, riktighet och spårbarhet.

Kursen ger kunskaper i/om:

- Hot, risk- och sårbarhetsanalys och potentiella angreppstekniker och hot mot IT-system
- Systemdokumentation för spårbarhet (dokumentation av kravanalys, design, implementation, test och drift av systemet)
- Agila processer och modeller för projektstyrning och IT-utveckling av IT-system med höga krav på säkerhet
- Förvaltningsmodeller, projektledningsmodeller och livscykelhantering
- Principer för hur man bygger flera lager av säkerhet kring ett system

Efter avslutad kurs ska den studerande ha färdighet att:

- Montera och konfigurera hårdvara för servrar och klienter samt annan väsentlig kringutrustning
- Utföra funktions- och säkerhetstester av IT-system
- Beskriva olika typer av kryptering, certifikat och trafikskydd

Efter avslutad kurs ska den studerande har kompetens att:

- Genomföra risk- och sårbarhetsanalys kopplat till IT-system i en given kontext/användningsfall
- Beskriva hur arkitekturen för IT-system med höga krav på informationssäkerhet bör utformas
- Föreslå säkerhetshöjande åtgärder kopplat till identifierade risker

IT-juridik (20p)

Syfte och mål:

Kursens syfte är att ge de studerande kunskap om de lagar, förordningar och regelverk som behöver tillämpas och följas inom IT-säkerhetsarbetet. Målet är att de studerande ska kunna resonera kring det pragmatiska förhållningssätt som krävs vid att förhålla sig till regelverk för verksamhet och samtidigt utföra handlingar inom yrkesrollen som ska vara etiskt försvarbara.

Kursen ger kunskaper i/om:

- När följande svenska lagar och regelverk är tillämpliga:
- Dataskyddsförordningen, GDPR och behandling av personuppgifter
- Lagen om behandling av personuppgifter vid Försvarsmakten
- Offentlighetsprincipen
- Offentlighets- och sekretesslagen
- Reglemente för Säkerhetsskydd och hantering av säkerhetsskyddsvärden
- NIS och NIS2 direktiven med krav på säkerhet för leverantörer av samhällsviktiga- och vissa digitala tjänster
- Förordningar för statliga myndigheter på IT-säk området
- Lagen om Offentlig Upphandling – LoU
- Lagen om Upphandling på Försvars- och Säkerhetsområdet – LUFS

Efter avslutad kurs ska den studerande ha färdighet att:

- Övergripande förstå när följande standarder, lagar och kravställningar skall tillämpas:
- SS-EN ISO/IEC 27000 standard för ledningssystem för informationssystem (LIS)
- IEEE standarder för utveckling och hantering av mjukvara över hela livscykeln
- ITU-T standard för fibernätverk
- IETF standarder för Ethernet och Internet
- PCI-DSS standard för elektroniska betalningar
- Offentlighetsprincipen
- Offentlighets- och sekretesslagen
- KSF (svenska försvarsmaktens krav på säkerhetsfunktioner i IT-system)

Efter avslutad kurs ska den studerande har kompetens att:

- Tillämpa IT-juridik i vardagligt arbete med hjälp av riktlinjer
- Avgöra när svensk lag gäller eller om leverantörer kan omfattas av annan lagstiftning, t.ex. CLOUD Act

LIA – lärande i arbete (100p)

Syfte och mål:

Syftet med LIA är att introducera och stärka den studerande i sin nya yrkesroll under handledning på en egenvald arbetsplats. Målet med LIA är att den studerande ska få en anställning hos LIA-företaget eller någon av dess samarbetspartners.

- Kursen ger kunskaper i/om:
- LiA-företaget och dess bransch
- Branschens struktur, tillväxt, trender och möjligheter/hot
- Den egna yrkesrollens arbetsuppgifter och ansvarsområden
- Närliggande yrkesrollers kompetenskrav
- Teamets uppbyggnad och struktur

- Kunder, finansiärer och andra intressenter
- Trender, utveckling och nya tekniker
- IT-säkerhet, nätverkskomponenter, driftövervakning och/eller operativsystemhärdning

Efter avslutad kurs ska den studerande ha färdighet att:

- Omsätta och fördjupa sina egna kunskaper kring IT-säkerhet och informationssäkerhet i arbetslivet
- Planera och genomföra säkerhetsarbete i skarp kontext
- Arbeta med IT-säkerhet, nätverkskomponenter, driftövervakning och/eller operativsystemhärdning

Efter avslutad kurs ska den studerande har kompetens att:

- I sin yrkesroll praktiskt tillämpa och fördjupa sig i de kunskaper som inhämtats under utbildningen

Nätverksteknik (50p)

Syfte och mål:

Kursens syfte är att ge de studerande teoretiska och praktiska kunskaper i nätverkskommunikation samt den utrustning, mjukoch hårdvara, som krävs för att upprätta och underhålla fungerande system och nätverk beroende på användningsområde. Målet är att de studerande ska få praktisera konfiguration av IT-system, installation och härdning samt tolkning av vanliga script-språk.

Kursen ger kunskaper i/om:

- IP-stacken, routing och hur datapaket beter sig
- Begreppet nätverkssäkerhet och dess användningsområden
- Nätverkstekniska funktioner och hur dessa kan utvecklas
- VPN-teknik, brandväggar, skillnaden mellan LAN/WAN och upprättande av nätverk
- Funktion och användning av routrar och switchar
- Dokumentation av nätverk
- Säkerhet i virtuella system
- Nätplanering, design och topografi

Efter avslutad kurs ska den studerande ha färdighet att:

- Genomföra felsökning och avhjälpande underhåll i driftsatta system
- Använda och anpassa nätverk
- Bygga och administrera nätverk med fokus på säkerhet
- Upprätta och granska brandväggar och VPN
- Montera och konfigurera routrar och switchar
- Felsöka nätverk i drift - Utföra nätverksövervakning, användning av nätverksadministrationsverktyg samt design och konfiguration av LAN/WAN.
- Felsöka IT-system

Efter avslutad kurs ska den studerande har kompetens att:

- Bygga, upprätta, använda och anpassa nätverk utifrån verksamheters behov
- Identifiera säkerhetsbrister i nätverk, samt utföra övervakning och kontroll av större nätverk

Operationell teknik (10p)

Syfte och mål:

Syftet är att introducera den studerande till industriell teknik, också kallat OT – Operational Technology, d.v.s. datorsystem för styrning och övervakning av industriella processer. Målet är att den studerande ska kunna analysera risker och sårbarheter i en verksamhet och ta fram förslag på åtgärder baserade på digital teknik kombinerat med mekaniska skydd och säkra arbetsmetoder i enighet med EUs förordningar.

Kursen ger kunskaper i/om:

- Aktuella lagkrav och förordningar kopplat till industriell teknik (OT), t.ex. NIS2 direktivet
- Standarder inom OT, som ISA/IEC 62443
- Vilka sektorer som omfattas av OT såsom samhällskritiska sektorer där konsekvenserna är stora vid felfunktion eller avbrott (t ex Kemisk tillverkning, Kommunikation och Transporter, Räddningstjänst, Energi, Livsmedelstillverkning, Hälso- och Sjukvård, Vattenrening, Kärnkraft)
- Skillnaderna mellan IT och OT
- Kontinuitetsplanering av OT-verksamheter: Dokumentation av system och status, Regelbundna funktionskontroller, Incidenthanteringsrutiner, Backup och avbrottshantering
- Exempel på risker och sårbarheter i sektorer som använder OT

- Viktiga begrepp inom OT såsom DCS (Distributed Control Systems) för distribuerad styrning, SCADA (Supervisory Control And Data Acquisition), PLC, Automation och IoT (Internet of Things)

- Efter avslutad kurs ska den studerande ha färdighet att:

- Redogöra för skillnader och likheter mellan IT och OT

- Redogöra för hur system och checklistor för OT kan appliceras i en tillverkande industri

- Redogöra för vad IT och OT har för synergier kopplat till cyber security metodik

Efter avslutad kurs ska den studerande har kompetens att:

- Undersöka vilka EU-förordningar som styr hur företag behöver hantera Operational Security

Säker molnstrategi (25p)

Syfte och mål:

Kursens syfte är att ge de studerande kunskaper i säkerhetsbrister kopplat till lagring i molntjänster. Kursen ger de studerande fördjupning i de hot och risker som finns vad gäller molnsäkerhet och hur dessa ska kunna åtgärdas. Målet är att de studerande ska kunna installera och hantera molntjänster ur ett säkerhetsperspektiv, samt hur de ska använda kryptering och signering och utföra identitetskontroller i molntjänster.

Kursen ger kunskaper i/om:

- Lagring i molntjänster

- Cloud security

- Inloggnings-och behörighetsmekanismer för molntjänster

- Säkerhet kopplad till ökad användning av digitalisering och molntjänster

- Infrastructure as a Service (IaaS) som är IT-infrastrukturella tjänster i nätet

- Platform as a Service (PaaS) som är applikationsplattformar via Internet eller annat nät

- Software as a Service (SaaS) som är färdiga eller konfigurerbara applikationer som tillhandahålls via Internet eller annat nät.

Efter avslutad kurs ska den studerande ha färdighet att:

- Beskriva funktion av molntjänst samt de vanligaste säkerhetsbristerna
- Installera och konfigurera säkra molntjänster
- Utföra behörighetskontroll kopplad till molntjänster
- Använda kryptering och signering i samband med molntjänster

Efter avslutad kurs ska den studerande har kompetens att:

- Skapa strategier för lagring av big data i molnet

Virtualiseringsteknik och automation (40p)

Syfte och mål:

Kursens syfte är att ge de studerande kunskaper och kompetenser på området virtualisering av datormiljöer. De studerande lär sig skillnader mellan fysiska och virtuella datormiljöer, olika metoder av virtualisering samt deras fördelar och nackdelar. Målet är att de studerande ska kunna tillämpa virtualisering för att skapa flera resurser på en enskild dator eller server.

Kursen ger kunskaper i/om:

- Virtuella IT-system och typer av lösningar
- Metoder för virtualisering: Automatisering av drift och övervakning
- Virtualiseringssäkerhet (virusskydd, säkerhetsuppdateringar och härdning)
- Skillnaden mellan virtualieringsmetoder som applikationsbaserade lösningar, containerbaserade lösningar och hypervisorbaserade lösningar

Efter avslutad kurs ska den studerande ha färdighet att:

- Arbeta med datorvirtualisering, nätverksvisualisering, programvaruvirtualisering samt lagringsvirtualisering med ett säkerhetsperspektiv
- Redogöra för fördelarna med virtualisering av datorer, nätverk, programvaror och lagring för att dela resurser
- Tillämpa virtualiseringstekniker för att bygga en virtualiserad dator- och nätverksmiljö
- Redogöra för hur vanliga säkerhetsskydd kan tillämpas i virtuella datormiljöer

- Upprätta automatiserade funktioner för drift och övervakning av system
- Implementera virusskydd, härdning och loggning i virtuella miljöer
- Efter avslutad kurs ska den studerande har kompetens att:
- Analysera behov av säkerhetsskydd i virtuella datormiljöer och hur olika typer av säkerhetsskydd kan upprättas och utvecklas för att möta verksamhetens behov
- Designa system för skalbarhet, robusthet och redundans, utan att göra avkall på säkerheten

Har du frågor om utbildningen?

Kontakta Yrkeshögskolan i Enköping

E-post: yh@enkoping.se

Telefon: 0171-62 50 76

Yrkeshögskolan i Enköping
Östra Järnvägsgatan 10, plan 1
745 37 Enköping

Kontakta oss
yh@enkoping.se
0171-62 50 76