Ny cybersikkerheds-uddannelse

Datatekniker med speciale i cybersikkerhed

Dansk Industri

DANSK METAL

Metalindustriens Uddannelsesudvalg

Erhvervsuddannelse med fokus på informations- og cybersikkerhed

Fra 2025 udbydes en ny cybersikkerhedsuddannelse i Danmark. Den nye erhvervsuddannelse **Datatekniker med speciale i cybersikkerhed** forbereder lærlingen på både teknisk drift og strategisk sikkerhedsarbejde gennem praktisk kunnen og teoretisk forståelse.

Med uddannelsen får lærlingen en omfattende viden og færdigheder inden for cybersikkerhed og informationsbeskyttelse. Gennem et struktureret læringsforløb fokuseres der på at implementere sikkerhedsløsninger, der beskytter organisationer og virksomheders aktiver i henhold til gældende lovgivning. Uddannelsen er opbygget omkring anerkendte standarder og værktøjer, som bidrager til struktureret governance og praktisk implementering af sikkerhed i systemer, netværk, servere, applikationsudvikling mv.

Virksomheden får en professionel, faglært cybersikkerhedstekniker. En lærling, der forstår både teknikken (SIEM, API'er, patching) og forretningen (Awareness, Trusselsvurderinger, Risici). En der proaktivt bygger og vedligeholder de digitale forsvarsværker i virksomheden.

Uddannelsens hovedområder:

- Proaktiv og reaktiv informations- og cybersikkerhed ud fra virksomhedens forretningsmål.
- Analyse, planlægning, implementering, drift og vedligehold af sikkerhedsløsninger i henhold til gældende standarder.
- Beskytte og overvåge it-systemer og programmer mod hacker-angreb og sikkerhedsbrud.

Kompetencemål i hovedforløbet

Uddannelsen i cybersikkerhed omfatter i alt **21 specialiserede kompetencemål.** Centrale områder inkluderer:

- Cybersikkerhed i praksis (fx implementering og drift af sikkerhedskomponenter i fx IoT, cloud, hardware og software samt overholdelse af ISMS og internationale standarder).
- Incident management og drift (opsætning og drift af SIEM og SOC, herunder logging, overvågning og incident response).
- Risikostyring (mitigation af risici, risikovurdering, trusselsanalyse).
- Awareness og organisatorisk sikkerhed.
- Etisk hacking og udvikling af sikker kode (analyse af angrebsvektorer og brug af sikkerhedsværktøjer).

I uddannelsen indgår også **12 fælles kompetencemål,** som er fælles for it-supporter og datatekniker med specialerne infrastruktur og programmering. Dette skal sikre en fagteknisk grundforståelse og viden inden specialiseringen målrettet cybersikkerhed.

Uddannelsens varighed og struktur

- Uddannelsen har en varighed på fem år inkl. grundforløb 2.
- 55 skoleuger fordelt på minimum seks skoleperioder, heraf syv uger til valgfag. Den resterende tid er i oplæringsvirksomheden.
- Uddannelsen kan gennemføres som **eux**.
- Der kan i uddannelsen ansøges om merit. For personer over 25 år kan varigheden være kortere.

Indhold

Fag på uddannelsen fra 1. august 2025

FAG	SKOLEFORLØB					
	1	2	3	4	5	6
Netværk I	■					
Computerteknologi	■					
It Service management I	■					
Serverteknologi	■					
Serveradminstration og sikkerhed	■					
Serverautomatisering I	■					
Serverteknologi – Linux		■				
Serverteknologi – sårbarhedsanalyse		■				
Netværk II		■				
Kundeservice		■				
Backupteknologi		■				
Informations- og cybersikkerhed 1 – Grundlæggende Principper	■					
Informations- og cybersikkerhed 2 – Risiko- og Sikkerhedsledelse		■				
Informations- og cybersikkerhed 3 – Avancerede Sikkerhedsteknikker			■			
Informations- og cybersikkerhed 4 – Compliance og Regulering				■		
Informations- og cybersikkerhed 5 – Fremtidens Sikkerhedsstrategier					■	
Informations- og cybersikkerhed 6 – Afsluttende						■
Endpoint security 1			■			
Endpoint security 2				■		
Endpoint security 3					■	
Network security 1			■			
Network security 2				■		
Network security 3					■	
Application security 1			■			
Application security 2				■		
Application security 3					■	
Detection and response 1-2				■		
Detection and response 1-2					■	
Data security 1-3			■			
Data security 1-3				■		
Data security 1-3					■	
Afsluttende projekt for cybersikkerhed						■
Valgfag, Sikkerhedsstandard og informationsledelsessystem						
Valgfag, Cloud sikkerhed II						
Valgfag, Etisk hacking						
Valgfag, CIS kontroller IT implimentering						
Valgfag, Cloudteknologi						
Valgfag, Cybersecurity Operations						
Valgfag, Netværkssikkerhed						
Valgfag, Sikkerhed: Cloud-løsninger						
Valgfag, Sikkerhed: Firewall						
Valgfag, Software-defined networking						

BEMÆRKNINGER TIL FAGTABELLEN:

- Fag markeret med blåt er fælles for enten IT-supporter, Datatekniker i infrastruktur og/eller Datatekniker i programmering.
  En nærmere beskrivelse af det faglige indhold i de fælles fag kan findes på hentdata.stil.dk/uddannelser
- Valgfagene er ikke fastlagt til bestemte skoleforløb.
- **Der tages forbehold for, at skolerne kan tilrettelægge skoleforløb og fag forskelligt.**

Fag for specialet Datatekniker med speciale i cybersikkerhed

Informations- og cybersikkerhed 1 - Grundlæggende Principper

Faglige fokusområder i faget:

- Grundbegreber: privacy, databeskyttelse, risikovurdering.
- Adgangskontrol- og passwordpolitik.
- Håndtering af interessekonflikter.
- Machine learning i trusselsidentifikation.

Målpinde i faget:

- Redegøre for nøglebegreber inden for informationssikkerhed og cybersikkerhed herunder privacy, databeskyttelse og trusselvektorer samt risikovurdering.
- Udarbejde en adgangskontrolpolitik til regulering af brugeradgang herunder en passwordpolitik.
- Redegøre for gængse interessekonflikter, herunder deres årsager og konsekvenser.
- Viden om, hvordan man ændrer, begrænser og håndterer konflikter.
- Viden om, hvordan machine-learning kan anvendes i for eksempel sikkerhedsovervågning til identifikation af trusler.

Informations- og cybersikkerhed 2 – Risiko- og Sikkerhedsledelse

Faglige fokusområder i faget:

- Formål med ISO 27001, ISO 27002 og CIS.
- Compliance, regulering og beredskabsplaner.
- Multifaktor-autentifikation.
- Fysisk sikkerhed og adgangskontrol.

Målpinde i faget:

- Kendskab til formålet med gængse sikkerhedsstandarder (fx ISO 27001 og ISO 27002) og har kendskab til relevante organisationer.
- Forklare begreberne compliance og regulering samt værdien af en beredskabsplan.
- Viden om multifaktor-authentificering, som kombinerer noget man ved, noget man har og noget man er.
- Anvende sin teoretiske forståelse for fysisk adgang og sikkerhed til at udarbejde implementeringsforslag.

Informations- og cybersikkerhed 3 – Avancerede Sikkerhedsteknikker

Faglige fokusområder i faget:

- Proaktiv cybersikkerhed og risikovurderinger.
- Cloud-sikkerhed og governance tools.
- Machine learning i SIEM og SOC.
- It-processer og sikring af automatiseringsløsninger.

Målpinde i faget:

- Anvende proaktiv informations- og cybersikkerhed, med udgangspunkt i virksomhedens overordnede forretningsmål, igennem anvendelse af informationsteknologier (it) og operationelle teknologier (OT) og under hensyn til virksomhedens størrelse og kompleksitet.
- Udarbejde en risikovurdering på en mellemstor virksomheds aktiver og processer og implementere en CIS kontrol og mitigerings tiltag.
- Forklare sikkerhedsgennemsigtighed inden for cloud computing.
- Anvende et governance, risk and compliance tool,
- Anvende CIA-modellens Fortrolighed, Integritet og Tilgængelighed.
- Beskrive hvordan machine learning-teknologier kan anvendes med eksisterende sikkerhedsløsninger, såsom SIEM systemer, XDR samt SOC.
- Anvende it-procesoptimering, fra reaktiv til proaktiv, med henblik på forbedring af it-processer ved at skifte fokus fra at reagere til at forebygge gennem bedre planlægning og forvaltning.
- Identificere sikkerhedskomponenter og -behov i automatiseringsløsninger og foreslå relevante cybersikkerhedstiltag til beskyttelse af OT/it-miljøer.

Informations- og cybersikkerhed 4 – Compliance og Regulering

Faglige fokusområder i faget:

- GDPR, etiske aspekter og compliance reviews.
- Kompromitteringsanalyse og cybersikkerhedsmodeller.
- Asset- og Lifecycle Management, ITIL Change Management.
- Designprincipper: redundans, elasticitet, netværksagilitet.

Målpinde i faget:

- Forstå GDPR og dets implikationer for informationssikkerhed samt etiske aspekter inden for cybersikkerhed.
- Beskrive SOC 2 og relationerne til gængse sikkerhedsstandarder (fx ISO 27001).
- Gennemføre en compliance review herunder evaluere tredjeparts compliance og sikkerhed (underleverandører).
- Forklare hvordan man genkender tegn på kompromittering i systemer og netværk herunder udføre en grundlæggende analyse af en sikkerhedshændelse for at bestemme, hvilken type kompromittering der er sket og kan udvikle en strategi til at forhindre fremtidige kompromitteringer.
- Anvende en cybersikkerhedsmodel, som cyber kill chain modellen, eller lignende, til at vurdere et system for mulige angreb.
- Anvende Asset- og Lifecycle Management omfatter versionering og bogførings-lovgivning for at holde styr på aktiver. Change Management (ITIL) processer for at håndtere og implementere ændringer effektivt i organisationer. Lifecycle Management implementere en cyklus af Plan, Do, Check, Act (PDCA) samt ITIL-principper for hele livscyklussen af produkter eller tjenester.
- Anvende design parametre som, redundans, skalerbarhed, elasticitet, og netværksagilitet, samt forstå cybersikkerhed udfordringerne ved fejldesign.

Informations- og cybersikkerhed 5 – Fremtidens Sikkerhedsstrategier

Faglige fokusområder i faget:

- IT/OT-sikkerhed og integration.
- OWASP og CVE for sårbarhedshåndtering.
- Design af SOC og adfærdsanalyse.

Målpinde i faget:

- Identificere og vurdere sikkerhedsmæssige udfordringer i samspillet mellem IT og OT og integrere løsninger i en tværfaglig kontekst.
- Anvende best practices fra standarder som OWASP og CVE for at forbedre sårbarheds-håndtering.
- Beskrive et Security Operations Center (SOC) og dets rolle i organisationen. Dette indebærer at definere designkrav til SOC, herunder integration af Security Information and Event Management (SIEM) og log management i forhold til virksomhedens behov inden for den specifikke sektor.
- Anvende metoder til overvågning af adfærdsmæssige mønstre.

Informations- og cybersikkerhed 6 – Afsluttende

Faglige fokusområder i faget:

- Emerging technologies og cybersikkerhed.
- Dokumentation af sårbarhedsanalyser.
- Konflikthåndtering og udvikling af handlingsplaner.

Målpinde i faget:

- Udforske emerging technologies og deres indflydelse på cybersikkerhed.
- Dokumentere resultaterne af sårbarhedsanalyser og præsentere dem for relevante interessenter.
- Samarbejde med interessenter for at finde fælles løsninger og evaluere eksisterende processer for konfliktløsning i organisationen.
- Udvikle en handlingsplan for håndtering af sikkerhedsbrud relateret til adgangskontrol, herunder reaktion på angreb i mikrosegmenter.

Endpoint security 1

Faglige fokusområder i faget:

- Identifikation og rolle af endpoints i organisationers sikkerhed.
- Trusler: malware, phishing, ransomware.
- Antivirus, EDR, SIEM, NAC og softwareopdatering.
- Endpoint Security Policy og BYOD-håndtering.
- Netværkssegmentering og SOC-overvågning.

Målpinde i faget:

- Forklare hvad endpoints er og identificere typiske endpoint-enheder såsom computere, mobiler og IoT, samt deres betydning i en organisations sikkerhedsstrategi.
- Beskrive og analysere almindelige trusler mod endpoints, herunder malware, phishing og ransomware, samt anvende trusselsmodellering til risikovurdering.
- Viden om, hvordan man kan implementere og vedligeholde grundlæggende sikkerhedspraksis for endpoints, såsom softwareopdatering, antivirus og antimalware-løsninger.
- Viden om, hvordan man kan vurdere og anvende skalerbare sikkerhedsløsninger og endpoint management-værktøjer til forskellige typer enheder.
- Anvende virksomhedens Endpoint Security Policy, herunder håndtering af BYOD, softwarebegrænsninger og adgangsregler.
- Forklare og anvende principper for netværkssegmentering og NAC-løsninger i forhold til endpoint-sikkerhed.
- Beskrive og anvende funktionerne i EDR, SIEM, XDR, samt SOC som led i overvågning og respons på endpoint-hændelser.

Endpoint security 2

Faglige fokusområder i faget:

- Kryptering, adgangskontrol og autentifikation.
- Sårbarhedsscanning og patch management.
- Mobile enheder, fjernadgang og VPN.
- Strategisk brug af tidligere hændelser.
- Server-management, NAC og netværkssegmentering

Målpinde i faget:

- Implementere teknikker til beskyttelse af endpoints, herunder kryptering, adgangskontrol, authentifikation samt evaluere og anvende EDR-værktøjer til detektion og respons.
- Udføre sårbarhedsscanning og patch management, samt anbefale passende sikkerhedsforanstaltninger.
- Anvende EDR, SIEM, XDR og SOC, samt beskrive hvordan disse systemer overvåger, analyserer og rapporterer data.
- Anvende sikkerhedspraksis for mobile enheder, fjernadgang og VPN-forbindelser, samt integrere erfaringer fra tidligere hændelser i strategisk arbejde.
- Anvende endpoint management til servere, NAC-løsninger og netværkssegmentering som led i sikring af endpoints.

Endpoint security 3

Faglige fokusområder i faget:

- Incident response-planer og rapportering.
- Loganalyse og EDR/SIEM/XDR-data.
- IoT-sikkerhed og endpoint compliance.
- Federated search og nye teknologier.
- Sikker BYOD, MDM og brugerinvolvering.
- Sikkerhedstræning og kommunikationsmateriale.

Målpinde i faget:

- Udvikle og anvende incident response-planer, samt dokumentere og rapportere sikkerhedshændelser relateret til endpoints.
- Overvåge og analysere endpoint-logs samt anvende data fra EDR, SIEM, XDR og SOC til at identificere mistænkelig aktivitet.
- Implementere sikkerhedsforanstaltninger og endpoint management for IoT-enheder.
- Forstå og implementere rammer for endpoint security compliance og tilpasse løsninger til forskellige typer enheder.
- Evaluere og implementere nye teknologier og metoder, herunder logopsamling og "just-in-time" søgning med federated search.
- Analysere sikkerhedsrisici og udvikle strategier for sikker BYOD, herunder anvendelse af MDM og sikkerhedstræning af medarbejdere.
- Planlægge og gennemføre sikkerhedstræning for brugere af endpoints, samt udarbejde kommunikationsmateriale.

Network security 1

Faglige fokusområder i faget:

- Grundsikkerhed på routere, switche og firewalls.
- Identifikation af netværksangreb og sårbarheder.
- IDS/IPS, TLS-dekryptering, alarmer og logning.
- Change Management og SD-Access teknologier.
- Læsning og fortolkning af netværkstopologier.

Målpinde i faget:

- Implementere grundlæggende sikkerhed på routere, switche, og firewall i et givet firmanetværk.
- Identificere forskellige typer netværksangreb og deres påvirkning på netværksinfrastrukturen og dens betydning for en organisations informationssikkerhed.
- Implementere firewall-løsninger til at filtrere uønsket netværkstrafik.
- Redegøre for principperne i IDS/IPS firewallteknologi herunder nødvendigheden af TLS-dekryptering.
- Redegøre for behovet for netværksmonitorering, alarmer og logning.
- Implementere en change-management procedure på infrastruktur i en given virksomhed.
- Kendskab til SD-Access teknologier som for eksempel 802.1X herunder begrebet Secure Access Services Edge (SASE).
- Viden om hvordan man kan læse, udarbejde og fortolke fysiske og logiske topologitegninger med fokus på cybersikkerhed og sårbarheder.

Network security 2

Faglige fokusområder i faget:

- VPN-konfiguration (SD-WAN, IPsec).
- IDS/IPS i firewall-konfiguration.
- Microsegmentering og Zero Trust.
- Adgangskontrol og WPA3-enterprise med 802.1X.

Målpinde i faget:

- Konfigurere VPN-forbindelser (SD-WAN) for at sikre fjernadgang til netværket, herunder kryptografiske teknologier for eksempel IPsec.
- Implementere og konfigurere en firewall løsning herunder anvende Intrusion Detection/Prevention systems (IDS/IPS) til at overvåge og reagere på sikkerhedstrusler samt redegøre for nødvendigheden af logning og alarmer.
- Redegøre for nødvendigheden af micro-segmentering, for at minimere angrebsflader, og for relationen til Zero-trust.
- Identificere og implementere bedste praksis for sikker adgangskontrol til netværksressourcer.
- Konfigurere sikkerhedsprotokoller som for eksempel WPA3 enterprise med 802.1X for trådløse netværk.

Network security 3

Faglige fokusområder i faget:

- Sårbarhedsscanning og penetrationstest.
- Incident response og trusselsstrategier (BYOD, social engineering).
- Udarbejdelse af sikkerhedspolitikker.
- Audits og netværks-sikkerhedsstandarder.

Målpinde i faget:

- Evaluere netværkets sikkerhed gennem sårbarhedsscanning og penetrationstest herunder evaluering af nødvendigheden af sikkerhedsopdateringer.
- Designe og implementere en plan for håndtering af sikkerhedshændelser

Application security 1

Faglige fokusområder i faget:

- Grundprincipper for applikationssikkerhed og typiske trusler.
- Sikker kodning og inputvalidering (forebyggelse af SQL Injection og XSS).
- Security by Design-principper.
- Patch-management og kendte sårbarheder (CVE).
- Introduktion til SIEM og OWASP.

Målpinde i faget:

- Beskrive grundprincipper for applikationssikkerhed og identificere typiske applikationstrusler.
- Viden om hvordan man kan implementere grundlæggende sikker kodning og inputvalidering med henblik på at forhindre angreb som SQL Injection og XSS.
- Forklare og anvende principper for 'security by design', herunder brug af designmodeller og segmentering.
- Viden om hvordan man kan etablere og vedligeholde sikker opdatering og patch-management med fokus på kendte sårbarheder (CVE).
- Kendskab til sikkerhedsstandarder, webprotokoller og værktøjer som SIEM og OWASP med henblik på at styrke applikationssikkerhed.

Application security 2

Faglige fokusområder i faget:

- Udarbejdelse af datasikkerhedspolitik og sårbarhedsstyring.
- Sikker autentifikation, sessionshåndtering og API-sikkerhed.
- Implementering af OWASP Top Ten og secure coding practices.
- Kryptografi, nøglehåndtering og QEC-keys.
- Sikkerhedstests i SDLC, herunder penetrationstest.
- Trusselsmodellering og analyse af tredjepartsafhængigheder.
- Netværkssegmentering og firewall-arkitekturer.

Målpinde i faget:

- Udarbejde en Datasecurity Policy og anvende sårbarhedshåndtering i et udviklingsmiljø.
- Anvende sikre autentifikationsmetoder, sessionshåndtering og API-sikkerhed for at beskytte applikationer.
- Implementere sikker softwareudvikling efter OWASP Top Ten og anvende Secure Coding praksis.
- Anvende kryptografi, key management og QEC-keys til at sikre data i hvile og under overførsel.
- Planlægge og gennemføre sikkerhedstests gennem hele softwareudviklings-livscyklussen (SDLC), inkl. enhedstest, funktionstest og penetrationstest.
- Udføre trusselsmodeller og analysere effekten af tredjepartsafhængigheder.
- Forklare og anvende netværkssegmentering og proxy/firewall-arkitekturer med henblik på at styrke cybersikkerhed.

Application security 3

Faglige fokusområder i faget:

- Anvendelse af sikkerhedspolitikker ved udvikling af sikre applikationer.
- Beskyttelse mod angreb vha. Web-Proxy, logging og penetrationstest.
- Fejl- og undtagelseshåndtering, Whitebox/Blackbox-test.
- Sikkerhedsrisici ved anvendelse af AI/chatbots.
- Dokumentation med Software Bill of Materials (SBOM) og Data Loss Protection (DLP).
- Design af sikkerhedsarkitektur for applikationer.

Målpinde i faget:

- Anvende og evaluere organisationens sikkerhedspolitikker ved udvikling og vedligeholdelse af sikre applikationer.
- Identificere og implementere foranstaltninger til at beskytte applikationer mod angreb, herunder brug af Web-Proxy løsninger, samt udføre logging, overvågning og penetrationstest.
- Anvende sikker praksis for fejl- og undtagelseshåndtering, samt teste software med Whitebox/Blackbox-metoder og vurdere sikkerhedsrisici ved anvendelse af AI/chatbots.
- Bidrage til sikkerhedsrevision og dokumentation, samt forklare og anvende Software Bill of Materials (SBOM) og Data Loss Protection (DLP).
- Forklare og designe sikker udvikling, herunder designmodeller og sikkerhedsarkitektur for applikationer.

Detektion og respons 1

Faglige fokusområder i faget:

- Proaktiv vs. reaktiv cybersikkerhed.
- Detektion og respons i organisationens sikkerhedsstrategi.
- Overvågning af netværk og angrebsidentifikation.
- IDS/IPS, SIEM og SOC-introduktion.

Målpinde i faget:

- Forklare forskellen mellem proaktiv og reaktiv cybersikkerhed samt betydningen af detektion og respons som en del af organisationens sikkerhedsstrategi.
- Viden om overvågning af netværker, herunder hvordan man identificerer almindelige angrebsmetoder og hvilke metoder, der anvendes til at opdage og analysere disse.
- Implementere og anvende teknologier som IDS/IPS samt SIEM og forstå funktionerne i en SOC-løsning til detektion og eskalering.

Detektion og respons 2

Faglige fokusområder i faget:

- Identifikation af indikatorer på kompromittering og loganalyse.
- Forensic-analyse og trussels-identifikation.
- Incident response og hændelseshåndtering.
- AI/ML og automatiserede responssystemer.
- Eskalering og intern/ekstern koordinering.

Målpinde i faget:

- Identificere indikatorer på kompromittering, anvende loganalyse og gennemføre forensic analyser for at identificere sikkerhedstrusler.
- Deltage i incident respons og efterbehandling af hændelser for at identificere roden til problemer og forhindre gentagelse af sikkerhedsbrud.
- Anvende AI og Machine Learning samt implementere automatiserede responssystemer med henblik på at styrke detektion og reaktionstid.
- Identificere hvornår tekniske hændelser og opgaver kræver eskalering, samt koordinere overdragelse til relevante specialister og samarbejdspartnere internt og eksternt.

Data security 1

Faglige fokusområder i faget:

- Datatyper, klassifikation, adgangskontrol og kryptering.
- GDPR og databeskyttelsesprincipper.
- Backupstrategier: 3-2-1-1-0-metoden, snapshots og replikering.
- Risikoanalyse og beredskabsplaner: DRP, IRP og BCP.
- Brugeruddannelse og sikkerhedspolitikker.

Målpinde i faget:

- Forklare og anvende centrale principper for datasikkerhed, herunder datatyper (primære/sekundære, struktureret/ustruktureret), klassifikation, adgangskontrol og kryptering, identificere adfærd hos ondsindede aktører og vurdere konsekvenserne af datatab for en organisation.
- Kendskab til relevante lovgivningsmæssige rammer, herunder GDPR og databeskyttelsesprincipper, samt forståelse for compliance-begreber som Zero Trust og AAA (authentication, authorization, audit, etc.).
- Kendskab til, hvordan man planlægger og dokumenterer backupstrategier og databeskyttelsesforanstaltninger, herunder 3-2-1-1-0-metoden, redundans og teknologier som snapshots og replikering.
- Kendskab til, hvordan man identificerer risici og udvikle tiltag gennem risikoanalyse og sammenkoble dem med Disaster Recovery Plan, Incident Response Plan og virksomhedens Business Continuity Planning.
- Forklare betydningen af brugeruddannelse og overvågning (herunder AI), samt bidrage til udformning af sikkerhedspolitikker og formidling af disse.

Data security 2

Faglige fokusområder i faget:

- Defense in Depth, Zero Trust, Least Privilege, Secure by Design.
- GDPR, NIS2, Cybersecurity Act, ISO/ISMS.
- Backup- og gendannelsesstrategier med versionskontrol.
- Klassifikation, trusselsmodeller og sikkerhedssoftware.
- Datasikkerhedsstrategier og evaluering af DRP, IRP, BCP.

Målpinde i faget:

- Anvende centrale sikkerhedsprincipper som Defense in Depth, Least Privilege, Secure by Design, Zero Trust og de fire A'er (administration, authentication, authorization, audit) i praksis.
- Forstå og anvende relevante lovgivningsrammer såsom GDPR, NIS2, Cybersecurity Act og ISO/ISMS-kontroller, samt diskutere krav til dataopbevaring.
- Planlægge og dokumentere backup- og gendannelsesstrategier, herunder identificere passende backup-miljøer, overvåge og teste procedurer samt anvende versionskontrol.
- Anvende databeskyttelsesteknikker og trusselsmodeller, klassificere data samt evaluere sikkerhedssoftware med henblik på at sikre følsomme data mod potentielle sårbarheder.
- Analysere og kommunikere datasikkerhedsstrategier, herunder DRP, IRP og BCP, samt vurdere konsekvenser af databrud, simulere angreb og udvikle sikkerhedsmetrics.

Data security 3

Faglige fokusområder i faget:

- IAM, 2FA/MFA, Security = Prevention + Detection + Response.
- Analyse og mitigation af datasikkerhedsbrud.
- Strategisk datasikkerhed: kommunikation, risikoanalyse, træning.
- AI, ML, UBA og monitoreringsværktøjer.
- Internationale principper e.g. ISMS, ISO 27001, DRP, IRP, BCP.

Målpinde i faget:

- Anvende og forklare centrale sikkerhedsprincipper og -modeller, herunder Identity and Access Management, 2FA/MFA, Zero Trust og "Security = Prevention + Detection + Response."
- Analysere og evaluere datasikkerhedsbrud og lovgivningsmæssige krav, herunder GDPR, HIPAA, bogføringsloven, og implementere relevante afbødnings(mitigerings) tiltag og politikker.
- Bidrage til organisationens strategiske datasikkerhed gennem risikoanalyser, forbedringsinitiativer, træningsprogrammer og kommunikation med ledelsen.
- Anvende og vurdere teknologier som AI, machine learning, UBA og automatiserede monitoreringsværktøjer til at styrke databeskyttelse og identificere sikkerhedsrisici.
- Arbejde med internationale standarder og organisatoriske rammer for datasikkerhed, herunder ISMS, ISO/IEC 27001, DRP, IRP og Business Continuity Planning.

CIS kontroller it-implementering, valgfag

Faglige fokusområder i faget:

- Identifikation af aktiver og software.
- Grundlæggende sikkerhedskonfigurationer.
- Kontoadministration og adgangsstyring.
- Sårbarhedsidentifikation og rapportering.
- Loganalyse.

Målpinde i faget:

- Identificere og dokumentere virksomhedens digitale aktiver og software.
- Analysere og implementere grundlæggende sikkerhedskonfigurationer på systemer og netværksenheder.
- Foretage kontoadministration og adgangsstyring i overensstemmelse med god praksis.
- Identificere, dokumentere og rapportere sårbarheder samt foreslå afhjælpende handlinger.
- Dokumentere og analysere logdata for sikkerhedsmæssige hændelser.

Cloud sikkerhed II, valgfag

Faglige fokusområder i faget:

- Identitetshåndtering og MFA i cloudmiljøer.
- Cloudbaseret overvågning og logning.
- Netværkssikkerhed i cloud.
- Identifikation af cloud-risici.

Målpinde i faget:

- Konfigurere grundlæggende identitets- og adgangskontroller i et cloudmiljø, herunder brugen af roller, politikker og multifaktorautentifikation.
- Aktivere og anvende cloudbaserede overvågnings- og logningsværktøjer til at identificere hændelser og analysere cloudaktivitet.
- Opsætte grundlæggende netværkssikkerhed i cloudmiljøer, herunder brug af firewalls, netværkssikkerhedsgrupper og VPN-forbindelser.
- Identificere almindelige sikkerhedsrisici i cloudmiljøer og udarbejde en kort teknisk rapport med forslag til forbedringer.

Etisk hacking, valgfag

Faglige fokusområder i faget:

- Planlægning og udførelse af penetrationstests.
- Sårbarhedsanalyse og rekognoscering.
- Dokumentation og etisk rapportering.
- Fokus på lovgivning og risikovurdering.

Målpinde i faget:

- Planlægge, afgrænse og udføre en penetrationstest, herunder definere mål, omfang og lovmæssige rammer.
- Udvælge og anvende relevante værktøjer til rekognoscering, scanning og identificering af sårbarheder.
- Gennemføre praktiske tests af fundne sårbarheder ved hjælp af kontrollerede angrebssimulationer og dokumentere resultaterne på en fagligt og etisk korrekt måde.
- Udarbejde og formidle en professionel rapport baseret på en penetrationstest, målrettet både tekniske og ikke-tekniske modtagere, med fokus på sårbarheder, risikovurdering og forbedringsforslag.

Sikkerhedsstandard og informationsledelsessystem, valgfag

Faglige fokusområder i faget:

- Standarder som ISO 27000-serien og ISMS.
- Risikovurdering og risikobaserede tiltag.
- Politikker og procedurer for informationssikkerhed.
- Anvendelse af GRC-værktøjer og audits.

Målpinde i faget:

- Identificere og anvende centrale begreber, principper og kontroller i gængse sikkerhedsstandarder (fx ISO 27000-serien), herunder formålet med et informationsledelsessystem (ISMS).
- Gennemføre risikovurderinger og planlægge sikkerhedstiltag baseret på en risikobaseret tilgang og krav fra interessenter.
- Udvikle, dokumentere og implementere politikker, procedurer og handlingsplaner for informationssikkerhed, herunder håndtering af sikkerhedsbrud og beredskab.
- Anvende GRC-principper og værktøjer til at styre projekter og sikre løbende forbedring af ISMS-processer med Plan-Do-Check-Act-modellen.
- Deltage i interne audits, bidrage til ledelsens gennemgang af informationssikkerheden samt styrke sikkerhedskulturen i virksomheden.


ACCESS DENIED
ACCESS DENIED

Oplæringsmål

Faglige områder som lærlingen skal gennemføre under oplæring i virksomheden.

Cloud-sikkerhed	Forstå sikkerhedsaspekter ved cloud-baserede tjenester og implementere delt ansvar mellem kunde og udbyder.
Proaktiv informations- og cybersikkerhed	Anvende proaktiv informations- og cybersikkerhed, med udgangspunkt i virksomhedens overordnede forretningsmål, igennem anvendelse af informationsteknologier (it) og operationelle teknologier (OT) og under hensyn til virksomhedens størrelse og kompleksitet.
Netværksarkitektur	Designe og implementere sikre netværksarkitekturer, herunder segmentering og beskyttelse mod trusler.
Sikker Kodning og Applikationsudvikling	Bidrage til sikre kodningspraksisser og forstå OWASP-principper for at identificere og rette sårbarheder i applikationer.
Firewalls og IDS/IPS	Installere og administrere firewalls samt intrusion detection/prevention systems for at sikre netværksgrænser.
IAM-løsninger	Designe og implementere identitets- og adgangsstyringssystemer, herunder multifaktorgodkendelse.
Overvågning med SIEM-værktøjer	Udføre overvågning og analyse af sikkerhedshændelser ved hjælp af Security Information and Event Management (SIEM) systems.
Sårbarhedsscanning og Penetrationstestning	Udføre sårbarhedsvurderinger og penetrationstest for at identificere og mitigere potentielle sikkerhedstrusler.
Backup-strategier	Designe og implementere robuste backup-løsninger ved brug af 3-2-1-1-0-strategien for databeskyttelse med Air-Gab.
Datasikring og Kryptering	Udføre anvendelse af krypteringsteknikker til at beskytte data i transit og i ro.
Incident Response	Udvikle, anvende og gennemføre hændelseshåndteringsplaner for effektivt at reagere på sikkerhedsbrud.
Lovgivning og Regulativer	Forstå og implementere krav fra relevante sikkerhedsstandarder og regulativer som ISO 27001, NIS2, CyberSecurity Act. og GDPR.
Benytte XDR-løsninger	Installere og integrere Extended Detection and Response for forbedret trusseldetektions- og responsfunktionalitet.
Server og PC Hardening	Udføre implementering af konfigurationer og praksisser for at minimere risikoen for serverkompromittering.
CRG-tools til Governance	Anvende Cyber Risk Governance tools til at styre og overvåge cybersikkerhedsrisici og overensstemmelse.
Netværks-sikkerhedspolitikker	Udvikle og håndhæve netværkssikkerhedspolitikker, der beskytter organisationens infrastruktur.
Operativ Systemsikkerhed	Installere og vedligeholde operative systemer med regelmæssig patching og sårbarhedsstyring.
Uddannelse og Bevidstgørelse	Bidrage til udvikling af programmer for medarbejdernes uddannelse og bevidstgørelse om bedste praksis inden for sikkerhed.
Regular Loggennemgang	Udføre regelmæssig gennemgang og analyse af logfiler for at opdage usædvanlige aktiviteter.
Tredjepartsrisiko	Udføre evaluering af og styring af sikkerhedsrisici forbundet med tredjepartsleverandører og -tjenester.
Sikkerhedsarkitektur	Bidrage til en omfattende sikkerhedsarkitektur, der omfatter alle lag af it-infrastrukturen, fra applikationer til netværk og databaser samt processer.
End Point Sikkerhed	Installere og konfigurere endpoint-sikkerhedsløsninger for at beskytte individuelle enheder mod malware og andre trusler.
Backup og Gendannelse	Udføre regelmæssig backup af kritiske systemer og data, samt planlægge og teste gendannelsesprocedurer for at sikre dataenes tilgængelighed efter et sikkerhedsbrud med Air-gab.
Risikovurdering	Bidrage til og udføre risikovurderinger for at identificere, analysere og prioritere sikkerhedstrusler og sårbarheder i organisationens infrastruktur.
Sikkerhedsretningslinjer	Udvikle og implementere sikkerhedsretningslinjer og standarder, der er i overensstemmelse med best practices og regulatoriske krav.
Trusselanalyse	Udføre trusselanalyser for at vurdere potentielle sikkerhedsrisici og udvikle strategier til at mitigere disse.
Sikkerhedstest	Gennemføre regelmæssige sikkerhedstests af systemer og applikationer for at identificere og afhjælpe svagheder.
Digital Forensics	Forstå principperne for digital forensics og kunne anvende disse i tilfælde af sikkerhedshændelser.
Overvågning	Forstå og udføre konstant overvågning af netværkstrafik, Server, Applikationer og Services for at opdage uregelmæssigheder og potentielle sikkerhedstrusler.
Sikkerhedshændelsesrapportering	Bidrage til oprettelse af strukturerede rapporterings-procedurer for håndtering af sikkerhedshændelser og sikre, at alle medarbejdere er bekendt med dem.
Årlig Sikkerhedsevaluering	Udføre årlige evalueringer af organisationens sikkerhedsprogram for at identificere forbedringsmuligheder og sikre overholdelse af standarder.
Asset Management	Bidrage og anvende samt implementere en effektiv asset management-struktur, der sikrer, at alle aktiver (hardware og software samt processer) registreres, overvåges og vedligeholdes med henblik på at minimere sikkerhedsrisici. Dette inkluderer klassificering af aktiver baseret på følsomhed og kritikalitet, samt sikring af, at alle aktiver har de nødvendige sikkerhedsforanstaltninger på plads.
Storage-sikkerhed	Bidrage til at designe og implementere sikkerhedsforanstaltninger for lagringssystemer, der sikrer data mod uautoriseret adgang, tab eller ødelæggelse. Dette inkluderer konfiguration af netværkslagringssystemer (NAS) og storage area networks (SAN) med tilstrækkelige sikkerhedsfunktioner.
Data Lifecycle Management	Implementere data og og generel lifecycle management af Hardware og Software, for at styre, hvornår data opbevares, hvordan de beskyttes, og hvornår de skal slettes.
Change Management	Forstå og implementere change management-processer for at sikre, at alle ændringer i it-systemerne gennemføres sikkert og kontrolleret. Dette inkluderer at følge etablerede procedurer for godkendelse, dokumentation og test af ændringer for at minimere risikoen for driftsforstyrrelser og sikkerhedsbrud.
Opdatering af Applikationer	Udføre regelmæssige opdateringer af applikationer og systemer for at sikre, at de er beskyttet mod kendte sårbarheder. Dette inkluderer planlægning og koordinering af opdateringer for at minimere digitale risici.
Whitelisting	Implementere whitelisting for at sikre, at kun godkendte applikationer og programmer kan køre på virksomhedens systemer, hvilket reducerer risikoen for malware og uønskede programmer.
Kodesikkerhed	Bidrage til forståelse for kodesikkerhed og udvikle metoder til at evaluere og forbedre sikkerheden i kode, samt sikre, at koden overholder branchens bedste praksisser bla. for test.
E-mail Filtrering	Installere og konfigurere e-mail filtreringsløsninger for at beskytte organisationen mod phishing, spam og malware, der kan komme via e-mail.
DNS Filtrering	Implementere DNS-filtrering for at forhindre adgang til skadelige websteder og sikre, at al DNS-trafik overvåges og kontrolleres for ondsindede anmodninger.
Modenhedsvurdering	Anvende modenhedsvurdering af organisationens cybersikkerhed for at vurdere effektiviteten af de eksisterende sikkerhedstiltag. Dette inkluderer at identificere forbedringsområder og anbefale skridt til at øge den.

Kompetencemål

Faglige kompetenceområder og slutmål, som lærlingen gennemfører på enten skolen og/eller i virksomheden under uddannelsen.

Fra bekendtgørelse nr. 177 af 08/02/2025, §4, stk. 1.

Fælles kompetencemål for data- og kommunikationsuddannelsen:

1) Lærlingen kan foretage installation og grundlæggende konfiguration af netværksenheder og fejlfinde på netværket i forbindelse med opbygning og vedligeholdelse af lokalnet.
2) Lærlingen kan indgå i forandringsprocesser ved optimering og effektivisering af produktioner.
3) Lærlingen kan instruere, vejlede og servicere brugere.
4) Lærlingen kan installere, opgradere, konfigurere og anvende et serveroperativsystem, herunder foretage bruger- og ressourceadministration samt installation og konfiguration af værktøjer og sikkerhed.
5) Lærlingen kan arbejde ud fra strukturerede metoder for levering af it-service.
6) Lærlingen kan udarbejde og anvende den til branchen hørende dokumentation, herunder på fremmedsprog.
7) Lærlingen kan koble relevant teori og metode til tilrettelæggelse, design, opgavenedbrydning, udførelse, implementering, evaluering og overdragelse af relevante arbejdsopgaver fra oplæringen.
8) Lærlingen kan installere, opgradere, konfigurere, administrere og vedligeholde netværksservere, herunder foretage fejlsøgning og fejlretning.
9) Lærlingen kan analysere sikkerhedsproblemer i et netværk, herunder designe, planlægge, implementere og opsætte sikkerhedsløsninger på et netværk.
10) Lærlingen kan anvende machine-learning teknologier og Artificial Intelligence (AI), herunder Large Language Models (LLM), som værktøj inden for uddannelsens jobområde og analysere værdien af eventuel automatisering og autonomi.
11) Lærlingen kan, med udgangspunkt i virksomhedens størrelse, anvende asset- og lifecycle-management, herunder løbende klassificering, test og evaluering af ovenstående assets, personer og processer.
12) Lærlingen kan anvende aktuel branchetilhørende faglitteratur samt relevante myndigheders nyhedskilder og threat assessment. indsamling af data fra forskellige datakilder, samt validering, sortering, samkøring og forbehandling af data.

Kompetencemål for datatekniker med speciale i cybersikkerhed:

42) Lærlingen kan identificere, analysere og implementere sikkerhedsforanstaltninger i softwareudvikling for at beskytte applikationer mod sårbarheder og trusler.
43) Lærlingen kan vurdere sammenhænge imellem og behov for proaktiv og reaktiv informations- og cybersikkerhed, med udgangspunkt i virksomhedens overordnede forretningsmål, igennem anvendelse af informationsteknologier (it) og operationelle teknologier (OT) og under hensyn til virksomhedens størrelse og kompleksitet.
44) Lærlingen kan redegøre for gældende lovgivning inden for fagområdet og overholde denne.
45) Lærlingen kan analysere og involvere sig i informations- og cybersikkerhedens etiske og moralske dimensioner, herunder privatliv, databeskyttelse og samfundsansvar, når der træffes beslutninger.
46) Lærlingen kan identificere misbrug relateret til informations- og cybersikkerhed ved sammenkøring af data, for eksempel Big-Data, og iværksætte mitigeringstiltag.
47) Lærlingen kan arbejde ud fra strukturerede metoder for levering af informations- og cybersikkerhed, herunder bidrage til organisationens politik og strategi, igennem anvendelse af et information security management system (ISMS) og best-practices for design-principper og -modeller.
48) Lærlingen kan beskrive datasikkerhed, herunder fortrolighed, integritet og tilgængelighed, som en central disciplin inden for cybersikkerhed, der beskytter data mod uautoriseret adgang, tab og misbrug.
49) Lærlingen kan varetage løbende udførelse af risikovurdering med henblik på identifikation, analyse, prioritering og eventuel mitigering af risici for virksomhedens assets, personer og procedurer.
50) Lærlingen kan varetage forandringsprocesser i eksisterende og fremtidige informations- og cybersikkerhedsløsninger samt bidrage i projekter.
51) Lærlingen kan, i overensstemmelse med standarder inden for informations- og cybersikkerhed, udvikle, dimensionere, installere, opgradere, konfigurere, fejlsikre, administrere, teste og vedligeholde kritiske og ikke-kritiske, sikkerhedskomponenter, herunder netværksenheder, Internet of Things (IoT), Industrial Internet of Things (IIoT), hardware, software og cloud-miljøer, samt udføre fejlsøgning og fejlretning på disse.
52) Lærlingen kan beskrive et security operations center (SOC) og udvælge, implementere, administrere og vedligeholde en passende log management platform, herunder en security information and event management (SIEM) løsning, for herefter at bruge log-informationer til analyse og planlægning af incident-response.
53) Lærlingen kan analysere risici i en infrastruktur, med særlig opmærksomhed på underleverandører, og heraf designe, planlægge og implementere sikkerhedsløsninger samt efterfølgende kontrol og optimering.
54) Lærlingen kan overføre sin teoretiske forståelse for fysisk sikkerhed til konkrete implementeringsforslag.
55) Lærlingen kan, vedrørende informations- og cybersikkerhed, identificere og handle på interessekonflikter under hensyntagen til hensigtsmæssig kommunikation og samarbejde.
56) Lærlingen kan dokumentere og afrapportere de etablerede og igangværende relevante løsninger, processer og sikkerhedshændelser, herunder bidrage til opdatering af politikker, procedurer og kontroller.
57) Lærlingen kan deltage i og bidrage til etisk hacking med henblik på identificering og mitigering af interne og eksterne angrebsvektorer under hensyntagen til standarder og best-practice.
58) Lærlingen kan bidrage til udvikling og gennemførelse af uddannelse og træningsscenarier, såsom awareness kampagner, til medarbejdere og kunder i relation til fysisk og logisk informations- og cybersikkerhed.
59) Lærlingen kan specialisere sig i ét eller flere af virksomheders konkrete informations- og cybersikkerhedskomponenter og processer.
60) Lærlingen kan identificere behov for, inddragelse og overdragelse af opgaver og sager, samt eskalering til interne og eksterne specialister.
61) Lærlingen kan bidrage til identificering af sikkerhedskomponenter i automatiseringsløsninger med henblik på at højne sikkerheden i disse samt identificere informations- og cybersikkerhedsrelevante automatiseringsbehov.
62) Lærlingen kan udarbejde en hensigtsmæssig backup og restore politik, samt implementere og kvalitetssikre disse for at bidrage til contingency planning policy.

Dansk Industri

DANSK METAL

Metalindustriens Uddannelsesudvalg