



Cybersäkerhet för programutvecklare

Cybersecurity for software developers

7,5 högskolepoäng

7,5 credits

Ladokkod: C1CY1A

Version: 1.2

Fastställt av: Utskottet för utbildningar inom bibliotek, information och IT 2024-01-03

Gäller från: VT 2024

Nivå: Grundnivå

Huvudområde (successiv fördjupning): Informatik (G1N), Datavetenskap (G1N)

Utbildningsområde: Naturvetenskap

Ämnesgrupp: Informatik/Data- och systemvetenskap

Förkunskapskrav: Grundläggande behörighet

Betygsskala: Underkänd, Godkänd eller Väl godkänd

Innehåll

Kursen behandlar teorier, aktuell forskning och praxis inom cybersäkerhet, ett område som fokuserar på skyddet av datorsystem, nätverk och data från digitala hot. Kursen lägger särskild vikt vid förebyggande säkerhetsåtgärder som syftar till att försvåra och hindra attacker. Dessa attacker utförs i syfte att skada, förstöra eller ändra digitala resurser som data eller programvara, att obehörigt erhålla tillgång till konfidentiell information, och/eller att olovligt utnyttja ett digitalt systems tjänster. Ett centralt tema i kursen är att skapa förståelse för cybersäkerhet ur ett sociotekniskt- och administrativt perspektiv. De tekniska aspekterna inriktar sig på säkerhetsåtgärder och verktyg för skydd av datasystem och nätverk. De sociala aspekterna fokuserar på organisatoriska faktorer, mänskligt beteende och utveckling av en effektiv säkerhetskultur. De administrativa aspekterna behandlar t. ex. lagstiftning, policyhantering och branschspecifika standarder.

Moment som ingår i kursen är:

- Grundläggande teorier och begrepp inom cybersäkerhet
- Grundläggande tekniker och protokoll för datakommunikation över internet enligt OSI-modellen
- Datasäkerhet
- Nätverkssäkerhet
- Nya hot och säkerhetsutmaningar
- Metoder för riskhantering
- Etisk respektive skadlig hacking
- Organisationens roll inom cybersäkerhet
- Lagstiftning och standarder inom cybersäkerhet.

Mål

Efter avslutad kurs ska studenten kunna, med avseende på:

Kunskap och förståelse

- 1.1 förklara centrala begrepp och teorier inom området cybersäkerhet.
- 1.2 beskriva grundläggande principer, metoder och tekniker relaterade till cybersäkerhet.
- 1.3 förklara de vanligaste säkerhetsutmaningarna inom cybersäkerhet.
- 1.4 redogöra för tekniker och protokoll inom nätverks- och transportsikten enligt OSI-modellen för internet.
- 1.5 förklara etisk hacking och skadlig hacking, samt redogöra för deras respektive syften och målsättningar.
- 1.6 beskriva konsekvenserna av cyberangrepp för en organisation.
- 1.7 beskriva vikten av en proaktiv säkerhetskultur i organisationer för att motverka säkerhetsrisker.
- 1.8 visa grundläggande förståelse för lagar och standarder inom cybersäkerhet.

Färdighet och förmåga

- 2.1 identifiera och särskilja mellan olika typer av cyberattacker.
- 2.2 utföra enkla riskanalyser genom att identifiera och beskriva olika typer av hot, sårbarheter och attacker.
- 2.3 genomföra enklare säkerhetsanalyser av system och nätverk, samt föreslå lämpliga förbättringsåtgärder.
- 2.4 demonstrera grundläggande säkerhetsåtgärder för skydd av datasystem och nätverk.
- 2.5 söka upp och redogöra för relevant praxis kopplat till trender inom cybersäkerhet.

Värderingsförmåga och förhållningssätt

- 3.1 kritiskt granska och värdera metoder och val av tekniker inom cybersäkerhetsarbete.
- 3.2 reflektera över programutvecklarens ansvar och agerande inom cybersäkerhetsarbete.

Undervisningsformer

Undervisningen på kursen består av:

- föreläsningar
- handledning i workshopsform
- handledning av laborationer

Föreläsningarna presenterar kursens teoretiska innehåll. Handledning sker för grupplaborationer, vilka utgör kursens praktiska innehåll. På varje workshop arbetar studenterna, under överinseende av lärare, med en större uppgift som sedan går igenom och diskuteras gemensamt.

Undervisningen bedrivs på svenska, men undervisning på engelska kan förekomma.

Examinationsformer

Kursen examineras genom följande examinationsmoment:

Tentamen: Individuell tentamen

Lärandemål: 1.1-1.8, 2.1, 3.2

Högskolepoäng: 3,5

Betygsskala: Underkänd, Godkänd eller Väl godkänd

Laboration: Säkerhetsverifiering av internetbaserade tjänster (gruppuppgift)

Lärandemål: 1.4, 2.2-2.5, 3.1

Högskolepoäng: 2

Betygsskala: Underkänd eller Godkänd

Laboration: Etisk hacking (gruppuppgift)

Lärandemål: 1.5, 2.2-2.5, 3.1

Högskolepoäng: 2

Betygsskala: Underkänd eller Godkänd

För betyget Godkänd på hel kurs krävs Godkänd på samtliga examinationsmoment. För betyget Väl Godkänd på hel kurs krävs dessutom Väl Godkänd på *Tentamen: Individuell tentamen*.

Då kursplanen ändras kommer student som önskar slutföra rester från ett kurstillfälle att examineras utifrån kursens nya innehåll och upplägg. Då kursen har upphört kan student som önskar slutföra rester följa hela eller delar av annan likvärdig kurs.

Om studenten har ett beslut/rekommendation om särskilt pedagogiskt stöd från Högskolan i Borås på grund av funktionsnedsättning, har examinator rätt att anpassa examinationen. Examinator har att utifrån kursplanens mål avgöra om examinationen kan anpassas i enlighet med beslutet/rekommendationen.

Studentens rättigheter och skyldigheter vid examination är enligt riktlinjer och regelverk vid Högskolan i Borås.

Kurslitteratur och övriga läromedel

Kurslitteraturen är på svenska och engelska.

Stallings, William & Brown, Lawrie (2018). Computer security: principles and practice. Fourth edition Harlow: Pearson (valda delar ca 500 sidor).

Ytterligare litteratur omfattande maximalt 300 sidor tillkommer enligt lärarens anvisningar.

Studentinflytande och utvärdering

Kursen utvärderas i enlighet med gällande riktlinjer för kursvärderingar vid Högskolan i Borås, där studenternas synpunkter ska inhämtas. Kursutvärderingsrapporten publiceras och återkopplas till deltagande och blivande studenter i enlighet med ovan nämnda riktlinjer, och ligger till grund för framtida utveckling av kurser och utbildningsprogram. Kursansvarig lärare ansvarar för att utvärdering enligt ovan genomförs.

Övrigt

Kursen ingår i Systemarkitekturutbildningen med inriktning mot programutveckling.