Mission Possible

Masterprojekt – Softwarekonstruktion
Aalborg universitet

Mikkel Krøll Christensen (20192499)
Camilla Mai Ryskjær (20192510)

Vejledere:
René Rydhof Hansen
Danny Bøgsted Poulsen

Antal anslag: 128.142

Indhold

Abstract

The need for training in IT security has never been higher than today and there is great demand for these skills in both the public and private sectors. When looking at the concept of IT security, it is often obvious to associate security with physical infrastructure, but security should already be taken into consideration during development of the actual software.

The vocational education within the scope of data and communication there are, in addition to IT support, also two specialisations. One focuses on infrastructure and the other on software development. A large number of the enrolled students come directly from primary school, which means that the students are quite young and not everyone meet the grade requirements of 02 in Danish and mathematics. Their lack of experience and professional level, makes it challenging in relation to teaching and learning.

We often see that students find it difficult to navigate through high levels of abstraction and they find it challenging to understand and use security concepts and models without having practical experience with the subjects in question. This is also supported by our two studies.

Giving the students practical experience in software security has proven to be a bit of a challenge, both because the security subject is a complex matter, and the students are inexperienced, and they tend to quickly lose concentration. Furthermore, we are subject to a pedagogical framework in relation to ZBC's didactic settings, which is based on problem-based learning and increased and instant feedback model.

This has made us want to investigate how to address software security in such a manner, that the students will have a more engaging and hands-on practice-based learning, which supports ZBC's didactic strategy.

To give our students practical experience and learning, we have developed an interactive learning platform from which students can train and test different "hacking" techniques in a closed and secure environment. To appeal to our students in general, we have designed and built our platform based on the concept of gamification and combined it with facts on what drives and motivates young people today, regarding their preferred learning processes.

Our platform “Mission Possible” gives our students lots of opportunities to test a large number of different attack vectors and subsequently learn about defence mechanisms, similar attack types, good principles and best practices. The platform is designed with the students' prerequisites in mind, both socially, mentally and their current experience with software development. The whole concept is built around exciting storytelling about agents, bandits and secret missions and the end goal is to save the world, and of course to learn about software security.

Læsevejledning

Denne masterrapport handler om en mere praksisnær tilgang til læring i forhold til softwaresikkerhed. Vi har både udarbejdet en masterrapport og et tilhørende produkt. Produktet består af en læringsplatform, som giver vores elever mulighed for at arbejde med "hacking", i et kontrolleret og afgrænset virtuelt miljø. Vi har valgt at præsentere produktet gennem følgende video https://youtu.be/LFbuziV1V7I.

Vi har sammen med denne rapport, vedlagt en ZIP fil (bilag.zip). Denne fil indeholder alle vores bilag, såsom kodebøger, opgavesæt og transskriberinger af interviews. Alle bilag er organiseret i mapper.

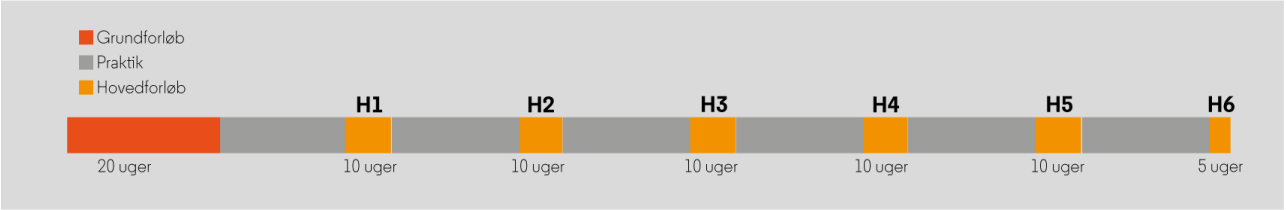
En erhvervsuddannelse er opbygget i hovedforløb, det vil sige perioder hvor eleven er på skole og vi refererer til hovedforløbene ved at angive H foran det hovedforløb eleverne er tilmeldt. Eksempelvis er H1 det samme som første hovedforløb.

Indledning

Vi er til dagligt undervisere på ZBC (Zealand Business College), som er en erhvervsskole. Vi underviser primært på uddannelsen som datatekniker med speciale i programmering. De faglige undervisningsområder spænder bredt fra både systemudvikling, projektledelse og til mere tekniske fagretninger indenfor programmering, både lav-og højniveau sprog og på mange forskellige teknologiske platforme.

Vi er begge uddannet datamatikere med en diplomuddannelse i programudvikling som overbygning, og inden vi overgik til "*lærergerningen*", har vi begge været ansatte som system- og softwareudviklere i en del år.

En erhvervsskoleuddannelse er en anden form for ungdomsuddannelse, set i forhold til den gymnasiale retning, og der er mange faktorer, som gør sig gældende indenfor erhvervsskoleregi. Der er mange, og indimellem modstridende, interessenter tilknyttet en erhvervsuddannelse, både industrien, fagbevægelsen, skolen, undervisningsministeriet, læreplads og elev. Uddannelsen, som datatekniker med speciale i programmering, er en vekseluddannelse, som fra start til slut tager mellem 5½ - 6 år, alt afhængig om eleven tager en studenterrettet påbygning (EUX) eller ej. En vekseluddannelse har det særlige karakteristikum, at eleven, udover at være tilknyttet en erhvervsskole, også har indgået et ansættelsesforhold (læreplads) med en virksomhed som regel efter et afsluttet grundforløb. Eleven veksler derfor mellem skoleophold og ophold i virksomheden. Et typisk skoleophold varer 10 uger, med en enkelt undtagelse af det sidste forløb, hvor eleverne udarbejder den afsluttende svendeprøve.



Figur 1: Standardiseret uddannelsesforløb datatekniker

Uddannelsen som datatekniker er ikke særlig udbredt, det skyldes muligvis at den er placeret under industriens uddannelser og betragtes som en håndværkeruddannelse. Kigger man på de overordnede rammer for uddannelsen, svarer mål og læring til den mere populære uddannelse "Datamatiker", og begge uddannelser er også placeret i samme kvalifikationsramme for livslang læring. (Uddannelses- og forskningsministeriet, 2020)

Den typiske datateknikerelev

En EUD[1] elev kommer typisk direkte fra folkeskolen, hvorimod adgangskravet på datamatikeruddannelsen kræver, at eleven har afsluttet en gymnasial ungdomsuddannelse. En typisk datateknikerelev er mand og mellem 18-23 år. Af erfaring ved vi, at mange af vores elever kommer med en del bagage fra folkeskolen, heriblandt diagnoser (Aspergers, ADHD og dysleksi)[2], lavt fagligt niveau og en generel skoletræthed. Erhvervsuddannelserne er generelt præget af denne type elever, hvilket stiller store krav til den didaktiske tilgang til gennemførelse af undervisning, hvilket også gives til kende i ZBC's overordnede (lærings)strategi i forhold til eleverne. Det overordnede mål er; at

[1] Erhvervsskoleelev
[2] Der findes ingen officielle tal, på hvor stor en andel af elever, som starter en erhvervsuddannelse, som har diagnoser, men lave adgangskrav og indførelse af FGU, gør det nemmere at blive optaget på en erhvervsuddannelse, fremfor andre ungdomsuddannelser

reducere den klassiske deduktive tavle undervisning til et minimum, og at eleverne i stedet skal være aktive og *"selvkørende*[3]*"* indenfor de første 5 minutter af en lektion.

Lærepladsen

En erhvervsuddannelse er styret gennem tre-parts aftaler mellem staten og arbejdsmarkedets parter. Eleverne indgår et kontraktuelt forhold med virksomheder og får løn under hele deres uddannelse og får betegnelsen lærling. På Sjælland er der kun to skoler, der udbyder hovedforløbsundervisning på vores område, hvoraf den ene er placeret i Ballerup, og den anden er ZBC i Ringsted. Som skole dækker vi derfor primært Vest- og Sydsjælland samt Lolland Falster. Vores placering har en stor indflydelse på, hvilke "mestre"/virksomheder vores elever har indgået uddannelsesaftale med. Mange af virksomhederne er meget små, ofte er der tale om enkeltmands- eller mikrovirksomheder. Disse typer af virksomheder kan være en udfordring for vores elever. Eleverne indgår, på godt og ondt og i langt højere grad, i hele udviklingsfasen fra indsamling af krav til implementering og drift, og flere elever er direkte ansvarlige for både softwaren og den underlæggende infrastruktur. Det betyder reelt, at eleverne i mange af disse virksomheder også er (med)ansvarlige for sikkerheden. Når eleven er i virksomheden, er der også en lang række praktikmål, som skal opfyldes. Disse mål er fastsat gennem industriens uddannelse og undervisningsministeriet i samspil med skolerne. Praktikmålene skal komplementere de faglige skolemål, og i kombination skal eleven tilegne sig en række kompetencer.

Skolen

For indeværende har vi 84[4] elever tilknyttet uddannelsen i Ringsted. For at blive optaget på selve hovedforløbet, skal eleven have gennemført grundforløbet på data og kommunikationsuddannelsen og have indgået en uddannelsesaftale med en virksomhed, alternativ skoleoplæring (UddannelsesGuiden, u.d.).

Den uddannelsesordning (Retsinformation, 2023) vi er tilknyttet, rummer omkring 400 færdighedsmål, fordelt på 27 obligatoriske fag, samt 7 ugers valgfrie specialefag[5], så alt i alt omkring 33 fag. Sammensætningen af fagpakker er defineret af arbejdsmarkedet (industrien) ud fra en behovsmæssig betragtning.

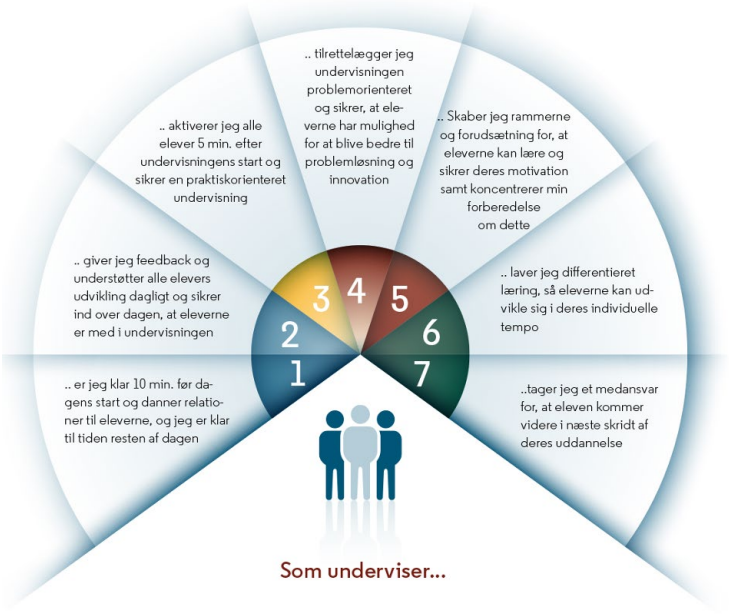
Som en del af erhvervsskolereformen skal alle skoler udarbejde et pædagogisk og didaktisk grundlag (ZBC, 2018). Dette grundlag definerer de overordnede rammer for, hvad skolen / direktionen ser som værende god undervisning.

Problemstilling

I forhold til samfundsdebatter, medier og den virkelighed vi befinder os i, ved vi, at behovet for at øge og sætte softwaresikkerheden på dagsorden er yderst nødvendigt, ikke kun i forhold til individet og persondata, men også set ud fra et økonomisk synspunkt. Ifølge en rapport fra Microsoft blev der i 2020 alene registreret og blokeret over 13 milliarder phishing-angreb på deres systemer (Microsoft, 2021) og Statista (Statista, 2022) anslår, at i 2027 vil cyber-angreb koste omkring 24 billioner dollars. I Danmark vurderer Center for Cybersikkerhed (Center for Cybersikkerhed, 2023) truslen mod danske myndigheder og virksomheder til at være høj, i forhold til cyberkriminalitet, og de antyder, at vores største problem er *ransomware*. De virksomheder, som vores elever er en del af, kan risikere at miste hele eller dele af forretningen enten i form af økonomiske sanktioner eller omdømme, hvis der opstår datalæk. Så der er ingen tvivl. Eleverne bør lære om sikker programmering og databeskyttelse for at

[3] Selvkørende betyder på ZBC at eleverne er i gang med praktisk arbejde, støttet af digitale læringsmidler og løbende feedback og feedforward af undervisere.
[4] Tallene er trukket i oktober 2022
[5] Svarende til valgfag

kunne udvikle software, som både beskytter sensitive informationer og som er mindre sårbare overfor angreb og udnyttelse af sårbarheder. Samtidig skal de også have viden om relevant lovgivning og regler, som kræves i forhold til, at softwaren overholder sikkerhedsstandarder og beskytter brugerdata. Vores grundlæggende ambition er, at vi gerne vil uddanne vores elever til at være sikkerhedsambassadører. Give dem viden, ballast og læring omkring sikkerhedsproblematikker, så de, når de returnerer til deres respektive lærepladser, kan være foregangsmænd og sætte sikkerheden på verdenskortet. Det er en svær og ambitiøs målsætning, for det har vist sig, at eleverne har svært ved at forstå sikkerhedsbegreber og deres abstraktionsniveau, hvilket blandt andet gives til udtryk i manglende forsvar- og sikkerhedsimplementeringer i deres kode. Eleverne er interesseret i sikkerheden, når det kommer til den praktiske del – de vil for eksempel gerne vide, hvordan man kan udføre et XSS angreb, men det skal vises i en praktisk sammenhæng, hvor de ser det ske, fremfor en beskrivende og teoretisk gennemgang.



Figur 2: ZBC Pædagogisk Didaktisk Grundlag 2020

På ZBC er der udarbejdet et fælles grundlag for god undervisning (se figur 2). Dette grundlag danner rammerne for, hvordan vi skal udvikle vores undervisningsmaterialer.

På ZBC gælder følgende *"regler"*. Undervisningen skal tage udgangspunkt i den enkelte elev, differentieret på baggrund af elevens niveau og være styret gennem facilitering og ad-hoc værkstedsundervisning. Rammen tager afsæt i, at ikke alle elever har brug for det samme. Derudover stilles der krav til digitaliserede undervisningsmaterialer og platforme.

Problemformulering

Hvordan kan vi, med afsæt i ovenstående, hjælpe vores relativt uerfarne elever til en mere engagerende hands-on og praksisnær læring, indenfor udvalgte dele af softwaresikkerhed, som understøtter ZBC's overordnede didaktiske grundlag?

Metode og teori

Vi har gjort brug af to kvalitative undersøgelsesmetoder til at blive klogere på elevernes opfattelse og deres praksis i forhold til softwaresikkerhed og har af den vej brugt undersøgelserne til at afprøve vores antagelser og udarbejde en mindre indholdsanalyse.

Da vores hverdag bærer præg af didaktik og læring hos vores elever, er det nærliggende også at inddrage elementerne indenfor læringsteorien og at tage udgangspunkt i vores elevers forudsætninger.

Undersøgelsesdesign

I de fleste af vores opgaver, i forhold til de sikkerhedsmoduler vi har gennemført på masteruddannelsen, har vores konklusioner omkring sikkerhedsbegreberne været, at viden er en afgørende faktor, når det kommer til sikkerhed - men er viden nok? Vi har igennem undervisningen haft langt højere fokus på sikkerheden, men sikkerhedsaspekterne er opstået i ad-hoc situationer og ikke været underlagt hverken faglige mål eller indgået i den didaktiske planlægning. Det har ofte resulteret i, at emner som f.eks. validering /sanitering og FIT modellen spontant er taget op i klassefællesskabet, og eleverne virker både interesseret og nysgerrige. Problemet opstår så efterfølgende, når vi skal vurdere og evaluere elevernes arbejde. Det viser sig ofte, at der ikke er synlige tegn på, at de har lært noget, og de har ikke implementeret retvisende sikkerhedsmekanismer.

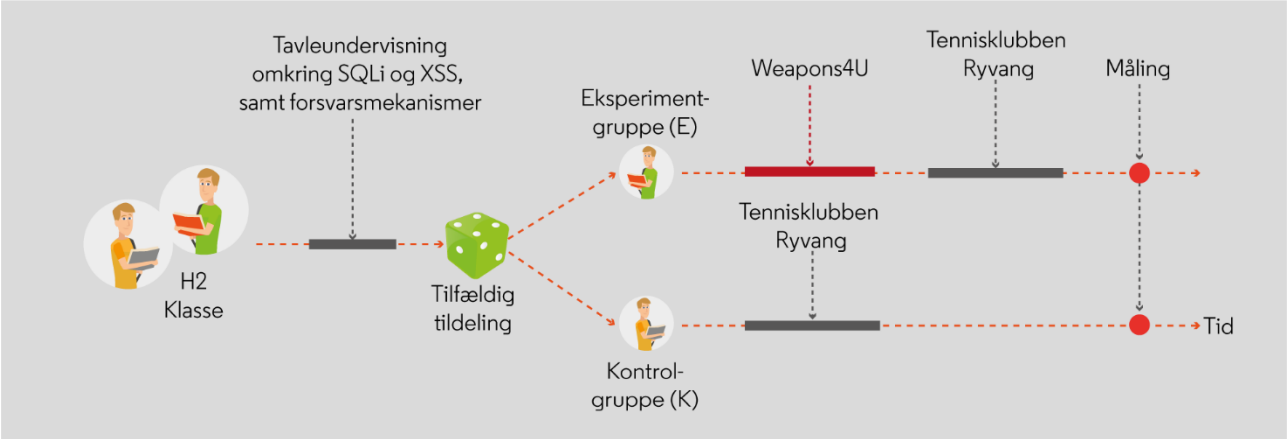
Vi er derfor meget nysgerrige på at tage temperaturen på elevernes nuværende sikkerhedsforståelse i forhold til, hvordan vi kan komme videre i forbindelse med vores problemformulering. Udover vores egen empiri, har vi valgt at gøre brug af to typer af undersøgelser, den ene er et eksperiment og den anden er interviews.

Eksperimentet

Eksperimentet vil undersøge, om teoretisk viden alene er tilstrækkelig til at implementere sikkerhedsforanstaltninger eller om praktisk erfaring også er nødvendig. Dette kan hjælpe med at identificere potentielle mangler i uddannelsen datatekniker med speciale i programmering, og informere om behovet for mere hands-on. Resultaterne kan også give indsigt i, hvordan man bedst kan integrere teoretisk viden og praktiske færdigheder for at opnå bedre sikkerhedsresultater. Det overordnede formål er at se og måle effekten på, om elever ændrer sikkerhedspraksis i takt med inddragelse af en mere praktisk orienteret opgaveløsning, som øger deres erfaringsniveau, fremfor elever, som kun stimuleres på viden og teoretisk baggrundsinformation. Dette har en indflydelse på, hvordan vi skal tilrettelægge og planlægge undervisningen.

Deltagerne i eksperimentet er en mindre H2 klasse med kun 13 elever. Eleverne er i begyndelsen af deres uddannelse, men har passende med programmeringserfaring til at kunne deltage i forsøget. Klassens generelle faglige niveau vurderes til at ligge omkring middel. Der er ingen, der skiller sig markant ud i forhold til programmeringskompetencer.

Vi har derfor valgt at udføre et 2-gruppe ægte eksperiment (Aarhus universitet, u.d.), bestående af en eksperiment- og kontrolgruppe. Forsøget foretages som et laboratorieforsøg i klasserummet for at sikre den interne validitet og hvorved vi kan kontrollere omgivelserne og nedtone eventuelle udefrakommende trusler. Grundet elevernes faglige udgangspunkt, har vi fravalgt at foretage en *pre-test* inden selve forsøget.



Figur 3: Eksperimentdesign

Forsøget vil strække sig over to dage. På førstedagen vil begge grupper modtage samme undervisning i samme lokale og på samme tid. Emnet vil være SQLi og XSS. Eleverne introduceres til begge emner gennem klassisk tavle undervisning (*Bilag Undervisningsmateriale*). Først vises forskellige typer af både SQLi og XSS-angreb, og hvordan de forekommer gennem de klassiske eksempler. Efterfølgende introduceres eleverne til forebyggelsesmekanismer såsom validering, sanitering og brug af parametriserede forespørgsler. Grundet eksperimentets længde er der kun fokus på disse få mekanismer.

Eleverne fordeles gennem lodtrækning, og de to grupper splittes til forskellige lokaler. Begge grupper skal løse opgaven "Tennisklubben *Ryvang" (Bilag Ryvang)*, som er en mindre opgave, der dækker UI til persistent lager. Kontrolgruppen får denne udleveret på førstedagen, eksperimentgruppen på anden dagen.

På et tidligere mastermodul udviklede vi et sårbart website Weapons4U (*Bilag W4U*) med tilhørende træningsopgaver i SQLi, som vi tidligere har gjort brug af i undervisningen. Opgavesættet er modificeret i sådan grad, at det også dækker både et "*reflected*" og "*stored*" XSS-angreb. Eleverne guides igennem en lang række øvelser, hvor de skal prøve at foretage forskellige typer af injektionsangreb. Opgavesættet er opbygget ud fra, at der først gives en teoretisk gennemgang eller beskrivelse af et typisk "*angreb*" og hvordan det kan undgås, og efterfølgende skal eleverne omsætte denne teoretiske viden til en praktisk tilgang og forsøge at løse en pågældende opgave.

Eksperimentgruppen får dagen efter udleveret samme opgave som kontrolgruppen. For begge grupper gælder det, at de skal løse opgaven indenfor rammen af 6 timer, og det står dem frit for, hvilket programmeringssprog og hvilken platform de ønsker at benytte.

Vi ønsker altså at måle effekten på elevernes udbytte af forløbet. Er der forskel på implementeringerne mellem kontrol- og eksperimentgruppe. Har det haft en *positiv* effekt på elevernes kode, at vi inducerer en "*A-ha*" oplevelse? Vi har fokus på følgende 3 hypoteser:

1. Hypotese
   Elever i eksperimentgruppen vil have en mere sikker tilgang i forhold til SQL-forespørgsler. De vil fravælge dynamisk SQL og i stedet bruge parametre i deres løsning. Kontrolgruppen vil derimod ikke have fokus på denne implementering.

2. Hypotese
   Eksperimentgruppen vil foretage inputvalideringen både på klient- og serversiden. Vi har en

formodning om, at kontrolgruppen kun foretager valideringen på klientsiden. Opgaven lægger op til, at eleverne både skal foretage semantisk og syntaktisk validering.

3. Hypotese
   I opgaven bliver eleverne bedt om at præsentere de data, som en fiktiv bruger kan have oprettet. Vi forventer eksperimentgruppen laver en form for output sanitering (*escaping* eller *encoding*) inden data præsenteres til klienten for at undgå XSS angreb.

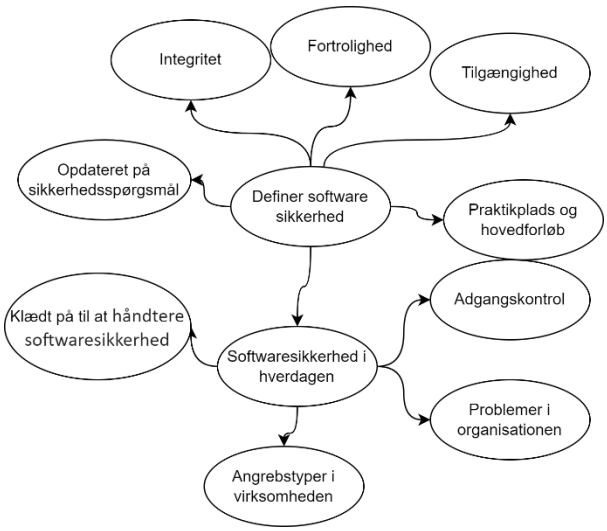
Der er potentielle trusler mod validiteten. Den ene er det, som refereres som værende en historisk trussel. Denne trussel kan opstå, når der indtræder en udefrakommende hændelse og i vores tilfælde kan det opstå, hvis og såfremt eksperimentgruppen får fortalt kontrolgruppen, hvad de arbejder med. Herved kan der opstå en refleksion i kontrolgruppen, der får dem til at ændre kurs. Som foranstaltning vil vi derfor forsøge at bygge en kinesisk mur mellem de to grupper og appellere til eksperimentgruppen om ikke at fortælle, hvad de arbejder med.

Da vi befinder os i et skolastisk miljø, er der fare for, at eleverne prioriterer deres besvarelse anderledes end vi forventer. Vores erfaring er, at eleverne ofte gerne vil vise os, hvor dygtige de er i forhold til abstraktionsniveau og generel kode-finesse. Eleverne er vandt til løbende evaluering og kan opfatte denne opgave, som en programmeringsprøve, hvilket kan betyde, at de fejlprioriterer og vælger at bruge tiden på f.eks. grafisk design eller implementering af designmønstre. Det skal derfor understreges tydeligt for eleverne, at deres løsning ikke har indflydelse på deres summative evaluering.

Interviewet

Vi har valgt interviews som en dataindsamlingsmetode af flere årsager. Vi har tidligere arbejdet med mere kvantitative indsamlingsmetoder i forhold til vores elever og de tidligere opgaver, vi har arbejdet med. Vi oplevede dog, at der var mange spørgsmål, som eleverne misforstod eller ikke kunne svare på, så vi har valgt at tage en mere kvalitativ tilgang til denne undersøgelse. Fordelene er, at under selve interviewet kan eleven spørge ind, hvis han eller hun er i tvivl om spørgsmålets betydning, og vi kan samtidig få mere detaljerede og nuancerede svar samt stille opfølgende spørgsmål.

I alt har 15 respondenter deltaget i vores interviews. Respondenterne er alle programmeringselever med praktikplads. De er alle mænd mellem 20-25 år og har minimum 1 års erfaring med softwarekonstruktion. Interviewene er semistrukturerede (Kristensen & Hussain , 2016). De udvalgte respondenter, hvis interviews vi anvender i det endelige datagrundlag, har været på skole i perioden marts til juni 2022. Vi har valgt at anvende semistrukturerede interviews som metode grundet vores relation til respondenterne. Vi ønsker ikke, at data skal baseres på hensigt eller selvrapportering. Formulering af de centrale spørgsmål i vores interviews med respondenterne tager afsæt i de tematiseringer, der er fremkommet gennem en brainstorm med udgangspunkt i uddannelsens mål, elevernes oplevelser i virksomhederne, de grundlæggende elementer i forhold til sikkerhed samt egne erfaringer.



Figur 4: Brainstorm i forhold til spørgeramme

Spørgsmål 1: Hvilke hovedforløb har du gennemført? (H1 til H6)?
Det kan være interessant at segmentere på, hvor i uddannelsesforløbet den enkelte elev befinder sig. En antagelse er, at elever, der er længere i uddannelsesforløbet, har en langt større forståelse af sikkerhedsbegreber på et abstrakt niveau fremfor elever tidligt i uddannelsen.

Spørgsmål 2: Er du ansat i en virksomhed eller tilknyttet skolepraktik?
Vi har en formodning om, at elever, som er tilknyttet skolepraktik (UddannelsesGuiden, u.d.) *har et langt mindre fokus på sikkerhedsbegrebet end elever tilknyttet en virksomhed. I skolepraktikken arbejder eleverne meget med "egne" opgaver, som aldrig skal leveres til en kunde eller udrulles til produktionsmiljøer.*

Spørgsmål 3: Hvordan definerer du begrebet softwaresikkerhed?
Dette spørgsmål skal være med til at afklare, hvordan eleverne opfatter begrebet softwaresikkerhed. Eleverne har tidligere været igennem en række server- og netværksfag, hvor sikkerhed, primært cyber-security, har været en del af undervisningen. Så det interessante er, om de har en forskellig opfattelse af sikkerhed mellem infrastruktur og software, og om de kan skelne mellem de to områder.

Spørgsmål 4: Når det kommer til softwaresikkerhed, hvor meget fylder det så i din hverdag og hos den virksomhed, hvor du er ansat?
Dette spørgsmål er interessant at høre svaret på både med afsæt i foregående spørgsmål, men også fordi vi er interesseret i at vide noget om sikkerheden i de organisationer, hvor eleven er ansat. Er der f.eks. en kausalitet mellem elevernes opfattelse og om, hvor meget det fylder i deres hverdag.

Spørgsmål 5: Har du oplevet, at I har haft problemer med sikkerhed i din organisation?
Som ved spørgsmål 4 er det interessant at vide, om der er kausalitet mellem, hvad eleverne oplever i deres virksomheder og til deres egen praksis. Har elever, der har oplevet problemer med sikkerheden i organisationen, en større forståelse og interesse i sikkerheden?

Spørgsmål 6: Hvor godt føler du dig klædt på til at håndtere softwaresikkerhed?
I nogle af vores tidligere undersøgelser i forbindelse med vores masteruddannelse, har vi haft gennemført en række interviews omkring sikkerhed. Flere af disse tidligere elever har givet udtryk for, at de mangler viden omkring sikre software implementering. Mange af vores elever er ansat i mikro- og startupvirksomheder, hvor der ikke er så meget sparring omkring sikkerhed, så flere føler, at de er overladt til sig selv, når det kommer til sikkerhedsimplementeringer.

Spørgsmål 7: Har du kendskab til, hvilke typer angreb jeres systemer kan udsættes for?
De fleste af vores elever har kendskab til en række angreb, men hvilke? Spørgsmålet skal være med til at afdække, hvor vi kan sætte ind. Hvis alle elever kender til XSS angreb og forsvarsmekanismerne, giver det ingen mening at dykke dybere ned i netop det emne, så er der muligvis mere værdi i at undersøge andre sårbarheder.

Spørgsmål 8: Hvad gør du får at holde dig opdateret på sikkerhedsspørgsmål?
Det er ekstremt interessant at se, om eleverne selv er pro-aktive i forhold til sikkerheden. Vi har flere gange oplevet, at eleverne efterspørger mere sikkerhedsundervisning, men tager de også selv et ansvar i forhold til at holde sig opdateret?

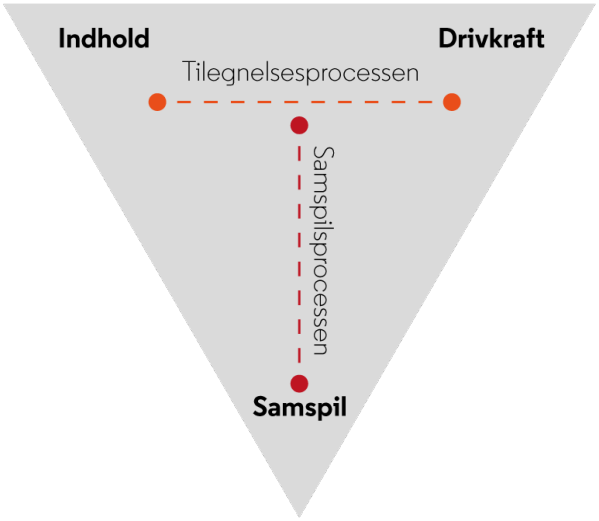
Spørgsmål 9: I den virksomhed du er ansat, arbejder I da med adgangskontrol i forhold til de systemer du er med til at udvikle? (Roller/ansvar). *Vi er interesseret i at vide, om eleven arbejder med adgangskontroller i de systemer, som vedkommende er med til at udvikle på sin praktikplads. Vi har stillet dette spørgsmål ud fra en antagelse om, at elever, som arbejder med adgangskontroller i hverdagen, også er bekendte med blandt andet FIT modellen og nogle af de angrebstyper, som retter sig*

direkte mod modellen.

Spørgsmål 10: Hvad er forskellen mellem integritet, fortrolighed og tilgængelighed? Hvorfor tror du, at det er vigtigt at vide?
Det kræver en vis grad af viden og forståelse for at besvare korrekt, hvilket kan være en udfordring for eleven. Spørgsmålet fokuserer på forskellene mellem integritet, fortrolighed og tilgængelighed, som er vigtige begreber inden for informationssikkerhed og afgørende for at opretholde softwaresikkerhed.

Læring og generation Z.

Da vi er undervisere, og læring fylder meget i vores hverdag, og vi kan se at svaret på vores udfordring eller problemstilling muligvis skal findes inden for læringsteorien, har vi valgt at gøre brug af Illeris' (Illeris, 2015) syntetiserede læringstrekant. Læringstrekanten er opbygget på baggrund af en række forskellige læringsteorier og skal være med til at give os en forståelse af, hvad og hvilke betingelser der skal opfyldes, for at eleven kan lære noget, både i forhold til individet selv, men også i samspillet med andre. Ifølge Illeris er der 3 dimensioner, som gør sig gældende i forhold til læring, og han ser læring som værende to sideløbende processer, hvoraf den ene er individets egen tilegnelsesproces, og den anden er samspilsprocessen med omverden.



Figur 5: Læringens tre dimensioner

Vi tænker, at mange svar kan findes i læringsteorien, men at den ikke kan stå alene. Elever, som vi underviser i dag, har nogle andre forudsætninger og krav til undervisningen, end de elever vi underviste bare for 6-7 år siden. Vi har derfor valgt at inddrage begrebet Generation Z i vores opgave for at se, om der i denne generation kan være nogle særlige udfordringer og karakteristika, vi skal være opmærksomme på i forhold til læring og Illeris' syntese. For at undersøge dette område nærmere, har vi vendt os mod Corey Seemiller og Meghan M. Grace, som nogle af de førende forskere indenfor Generation Z. Deres undersøgelser tager udgangspunkt i amerikanske studier af den unge generation, hvilket ikke nødvendigvis kan overføres direkte til danske erhvervsskoleelever. Vi vælger derfor at supplere Seemiller og Grace med uddrag af en række eksperters bud på "*unges lyst til læring*" (Katznelson, Sørensen, & Illeris, 2021).

Gamification

I forhold til, at vi ønsker at skabe et produkt, som er både praksisnært, og som tager udgangspunkt i "hands-on", har *gamification* været med som en del af vores overvejelser og implementering. For os, handler det ikke om at bygge noget på baggrund af konceptet "*Gamification*", det er altså ikke målet i sig selv, men skal mere ses som et middel til at opnå vores mål. *Gamification* handler kort og godt om, at anvende spildesignelementer og principper i ikke-spilrelaterede sammenhænge. Konceptet *Gamification*, som vi kender det i dag, har eksisteret siden 2010, men der findes ingen helt klar og tydelig definition på konceptet, det afhænger af, hvem du spørger, men Gartner.com giver et bud på en definition: "*The use of game mechanics and experience design to digitally engage and motivate people to*

achieve their goals." (Gartner, u.d.). Stikker man et spadestik dybere, så defineres *Game mechanics* som værende nøgleelementer, vi kender fra computer- eller brætspil som f.eks. *points*, *badges* og *score-boards*. Experience design beskriver selve rejsen spilleren skal på i form af eksempelvis et *gameplay* eller *storyboard*. Konceptet bag *gamification* handler i bund og grund om at *"lege"* sig til ny viden eller adfærd gennem motiverende aktiviteter og spil på en eller flere digitaliserede platforme. Som udgangspunkt har vi gjort brug af Burkes definition og vurdering af gamification og hans designstrategi (Burke, 2016) i forhold til implementering af vores platform. Vi har dog taget en kunstnerisk frihed i at omformulere enkelte af hans processer, så der tages udgangspunkt i et læringsmiljø fremfor en mere virksomhedstilpasset tilgang.

Figur 6: Design flow gamification

Sikkerheden

Opgaverne, som ligger i selve platformen, er designet med baggrund i en eller anden type kendt angreb eller sårbarhed, så når det kommer til softwaresikkerheden gør vi brug af flere forskellige metoder, principper og kilder. Som udgangspunkt har vi dog valgt primært at benytte OWASP og NIST's anbefalinger i forhold til konkrete implementeringer af forsvarsmekanismer. Når opgaverne drejer sig om dannelse, og *"de gode vaner"*, har vi mere set på Merkow og Raghavens gode principper for sikker softwareimplementering (Merkow & Raghaven, 2010).

Dataanalyse

Som resultat af vores undersøgelser har vi foretaget to struktureret indholdsanalyser. Når vi vælger denne tilgang, er det fordi interviewene er baseret på en række delvis lukkede spørgsmål og selve gennemførelsen af interviewene ikke gav mange yderligere oplysninger end svar på de konkrete spørgsmål. Under eksperimentet var vi kun fokuseret på resultatet af elevernes besvarelse, og der blev ikke foretaget andre observationer som for eksempel elevernes tilgang til materialet eller deres arbejdsmoral. Kodebøger til de to indholdsanalyser er vedlagt bilag (*Bilag Kodebog*). Ligeledes er transskriberinger af interviewene, i anonymiseret form (*Bilag Transskribering*), og elevernes kode fra eksperimentet (*Bilag Eksperimentet)* vedlagt bilag.

Resultatet af eksperimentet

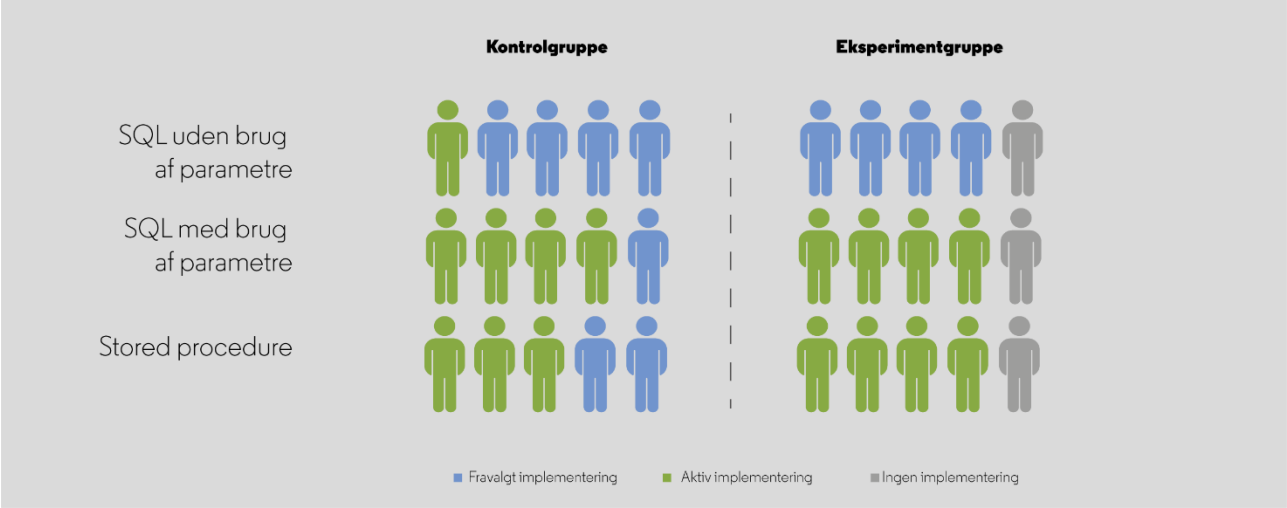
Datagrundlaget for vores eksperiment er relativt lille, og variationer har derfor stor betydning for selve resultatet. Vi startede med 13 elever, dette blev dog reduceret, grundet sygdom, til kun 10 testpersoner fordelt med 5 elever i hver gruppe.

Hver elevs kode blev gennemgået med tættekam, og for hver disciplin/*kategori* blev elevens kode individuelt vurderet. I forhold til databasehåndteringen grupperes elevernes løsning i 3 kategorier. En kategori, som angiver om eleven foretager SQL uden parameterhåndtering, en kategori med parametre og slutteligt en kategori i forhold til *stored produceres*.

I forhold til valideringen er der sat to kategorier, én til *client-side* og en for *server-side* validering. Elevernes løsning vurderes fra en skala fra 0-3. Hvor 0 angiver ingen validering og 3 angiver, at eleven har implementeret meget validering.

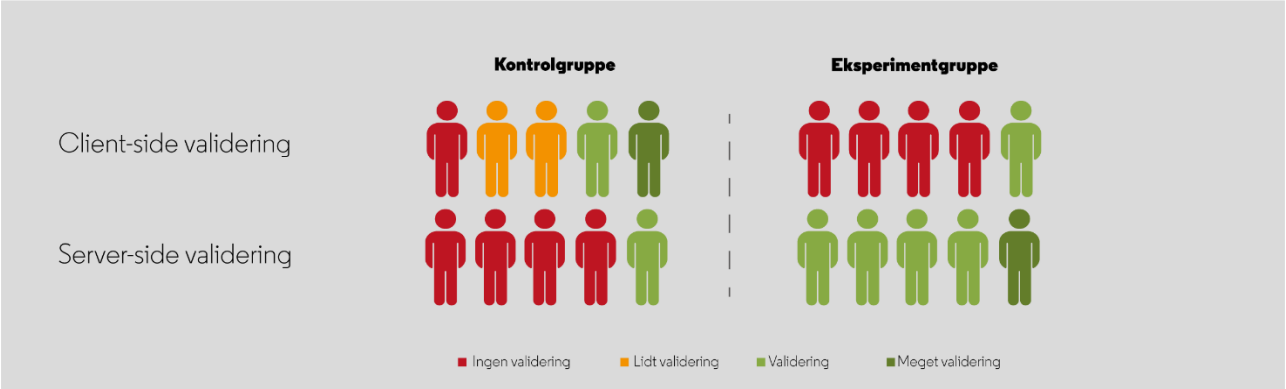
Overordnet set havde vi været for optimistiske i forhold til, hvor meget eleverne kunne nå på 6 timer. Ingen af de 10 elever nåede at implementere muligheden for at præsentere data, og derfor har vi ikke kunne validere, hvorvidt eleverne kan håndtere og implementere output sanitering i forhold til XSS-angreb. Endvidere havde vi ikke tydeliggjort rammerne for opgaven overfor eleverne, da én elev i eksperimentgruppen valgte at gøre brug af et *ORM* (*Object Relational Mapping*) framework.

I kontrolgruppen var der én elev, som potentielt var sårbar overfor SQLi. 4 elever ud af 5 havde valgt at bruge parametriserede forespørgsler, og 3 af disse 4 havde endvidere gjort brug af *stored procedures*. I eksperimentgruppen havde alle, på nær den elev, som havde valgt ORM, brugt både parametriserede forespørgsler i kombination med *stored procedures*.



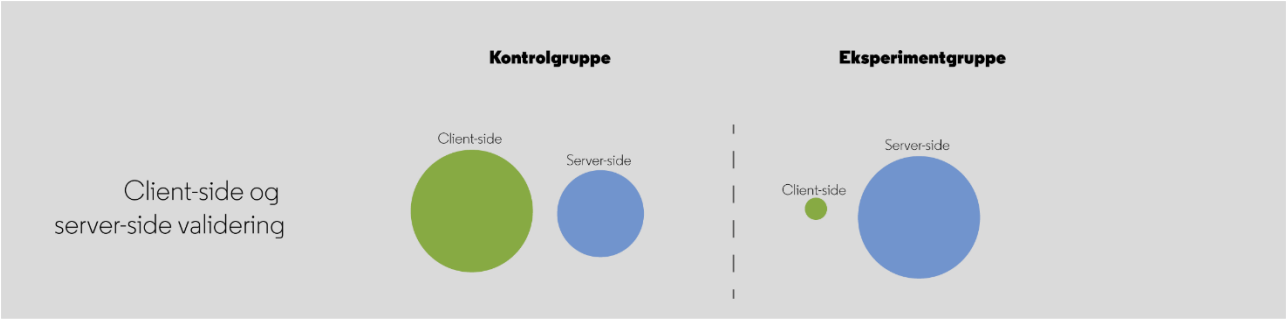
Figur 7: Elevernes SQL-håndtering

I forhold til validering af *tainted* input, ser resultatet mellem de to grupper mere varieret ud. 4 elever i kontrolgruppen havde implementeret dette. En elev, i kontrolgruppen, havde implementeret meget og en anden, intet. Det samme gjorde sig gældende i forhold til *server-side* valideringen. Her var der dog to, som valgte ikke at implementere nogen former for validering. I eksperimentgruppen har der været et fokusskifte. Noget kunne tyde på, at eleverne i denne gruppe, i forhold til kontrolgruppen, har brugt tiden på at implementere mere *server-side* validering fremfor *client-side*. Ingen af grupperne har valideret input i deres *stored procedures.*



Figur 8: Forskelle mellem client-side og server-side validering

Vi mener, at se en tendens, som peger i retning af, at eksperimentgruppen har haft større fokus på selve *server-side* valideringen og har nedprioriteret *client-side*. Noget af det vi gerne ville undersøge, var om eleverne ændrede fremgangsmåde i forhold til validering baseret på den praktiske erfaring med materialet.



Figur 9: Fordeling i forhold mellem client-side og server-side validering

Selvom datagrundlaget er relativt begrænset, og da vi ikke har gjort meget for at sikre den eksterne validitet, vil vi mene, på baggrund af vores eksisterende viden, at eleverne, i kontrolgruppens handlinger, afspejler en generel tendens. Det udsagn bakkes blandt andet op i statistikkerne. Bare i 2022 var 33% af alle web-applikationsangreb baseret på SQLi (Statista.com, u.d.), og injektionsangreb er stadig på OWASP top-10 over sikkerhedsrisici forbundet med webapplikationer.

Flere elever havde brugt parametriserede forespørgsler, men at stort set alle elever havde gjort brug af *stored procedures* kom som lidt af en overraskelse. Efter lidt puslespilsarbejde viser det sig, at eleverne, lige inden forsøgets start, havde haft et databasefag, hvori *stored procedures* var en del af pensum.

Resultatet af interviews

Alle elever, som har deltaget i undersøgelsen, har et ansættelsesforhold i en virksomhed, derfor udgår spørgsmål 2. Spørgsmål 9 udgår ligeledes, da det i, vores optik, ikke har relevans i forhold til det, vi gerne ville undersøge. Det sekundære spørgsmål i spørgsmål 10 udgår også, da det ikke har givet mening i forhold til elevernes besvarelser.

På baggrund af det indsamlede materiale har vi opdelt elevernes svar i 3 hovedkategorier; begrebsdefinitioner, sikkerhed på arbejdspladsen og sluttelig sikkerhedsambassadøren.

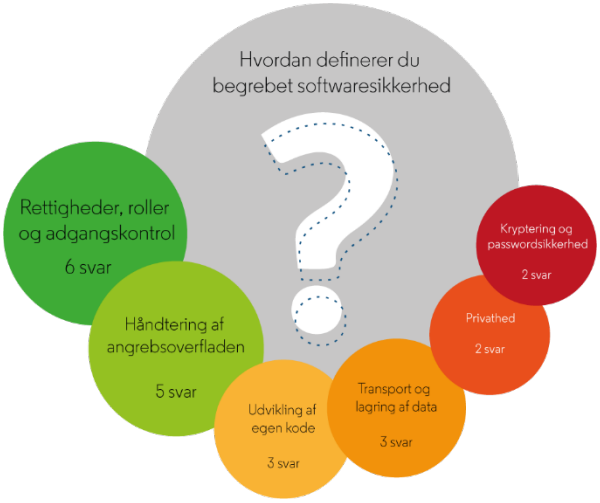
Begrebsdefinitioner

Så hvad dækker begrebet softwaresikkerhed så over? Det kan virke som et bredt begreb, for elevernes udtalelse er meget varieret og flere kommer med indtil flere bud på en definition. Vi har, efter en grundig gennemgang og analyse af data, kategoriseret elevernes besvarelser ind til 6 overordnede segmenter.

Elevernes svar er meget konkrete, og ingen kommer helt ind i kernen til den definition vi søger:

"Et systems evne til at opfylde sine mål i en modstanders tilstedeværelse"[6]

En enkelt elev definerer dog begrebet som værende *"Et sikkert program"*. Mange af deres svar tager afsæt i forsvarsmekanismer - altså hvordan man sikrer sin software mod uautoriseret adgang, og ord de kender som kryptering, hashing og passwordsikkerhed. 5 elever kategoriserer softwaresikkerhed som noget, hvor man skal mindske åbninger i forhold til angrebsoverfladen og gøre systemet så skudsikkert som muligt.



Figur 10: Elevernes opfattelse af softwaresikkerhed

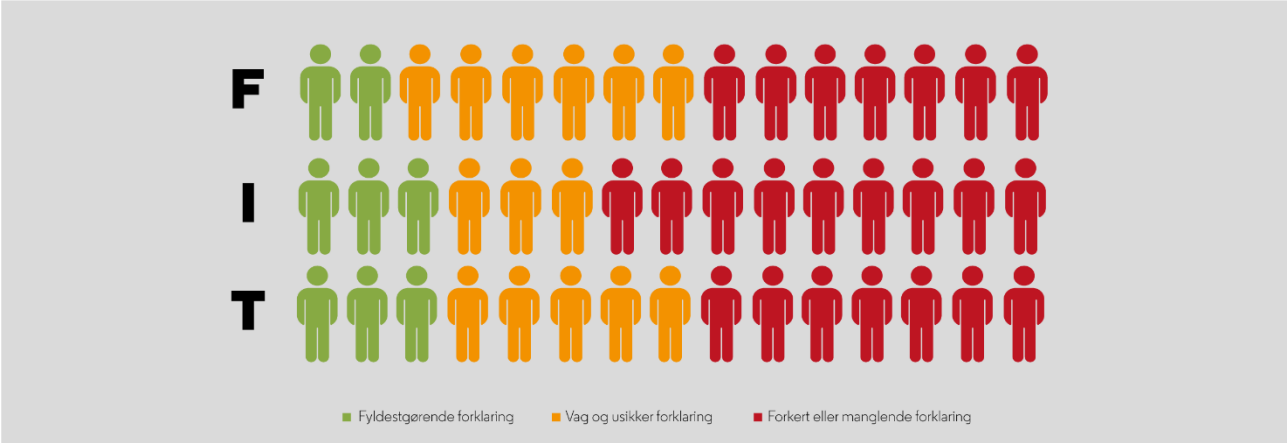
2 elever mener, det omhandler privathed. 6 mener, begrebet handler om at give de rigtige rettigheder, roller og adgang til systemer. 3 elever nævner endda deres egen kode og ser softwaresikkerhed, som noget, man aktivt selv skal implementere i egen kode. En elev nævner, at sikkerheden dog er *"noget"* man først implementerer, når systemet er helt færdigt, og en anden indikerer, at softwaresikkerheden i begyndelse af udviklingsprocessen ikke er så vigtig.

Der er mange gode bud på begrebet, og det er tydeligt at se, at eleverne er meget konkrete i forhold til deres besvarelser. Det interessante er at se flere nævne autorisation og autentificering som værende en del af definitionen på softwaresikkerhed. Dette kan muligvis skyldes, at eleverne tidligere har haft Microsoft serverfag, som retter sig mod brugerrettigheder, roller og adgang på et Windows domæne. Antagelsen bakkes op af, at det primært er elever på de første par hovedforløb, som har denne betragtning.

> *Jeg vil nok definere det som … at udefrakommende ikke kan få adgang til ressourcer, som vi ikke ønsker, de skal have adgang til.*
>
> *Citat: datateknikerelev*

Til spørgsmålet om definition på fortrolighed, integritet og tilgængelig er der 5 elever, som slet ikke kan beskrive eller formulere bare et af begreberne. Vi har vægtet elevernes udsagn i 3 kategorier. De kan enten ikke svare, eller de svarer forkert, de er vage i deres forklaring og slutteligt, at de svarer korrekt om end deres udsagn ikke overholder officielle definitioner.

[6] René Rydhof Hansen / siksoft02.pdf



Figur 11: Elevernes begrebsforståelse i forhold til FIT modellen

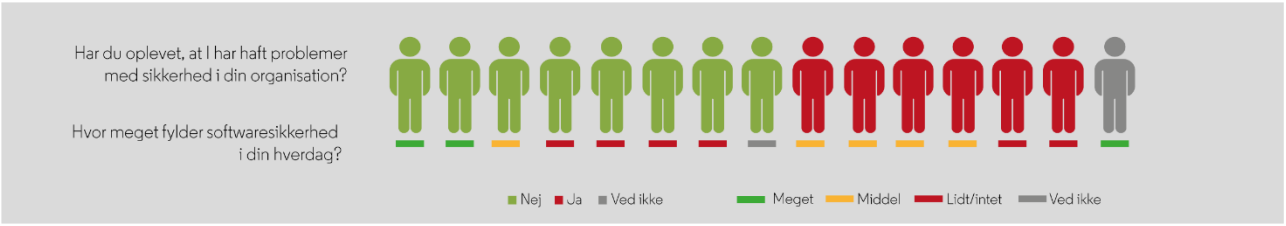
Ingen af de 15 elever kunne definere alle 3 begreber. Hvilket hovedforløb; eleverne er tilknyttet, har ingen betydning i forhold til deres svar. De to elever, som har svaret mest *korrekt* er tilkoblet en H2 eller en H3 klasse, hvorimod de to elever på sidste hovedforløb (H6) faktisk ikke kunne definere nogle af begreberne.

Sikkerhed på arbejdspladsen

Ser vi på elevernes hverdag ude i virksomheder, kan man formode, at sikkerheden har en central rolle i forhold til hverdagen, men noget tyder på, at situationen er anderledes. Til spørgsmålet om, hvor meget softwaresikkerheden fylder i hverdagen, er der kun 2 elever, ud af 15, der svarer, at sikkerheden fylder meget, hvorimod 6 svarer, at intet fylder eller i givet fald meget lidt. Vender man tilbage til elevernes opfattelse af softwaresikkerhed som begreb, og kombinerer det med elevernes svar på, hvor meget softwaresikkerheden fylder, er der ingen kausalitet. Man kunne have forestillet sig, at eleverne havde givet udtryk for, at softwaresikkerheden ikke fyldte meget, fordi de f.eks. betragtede softwaresikkerhed som noget med adgangskontrol, roller eller rettigheder og at der, i de systemer, de udvikler på, ikke indgår disse elementer, men det er ikke tilfældet.

Figur 12: Hvor meget fylder softwaresikkerheden

Samtidig er det interessant, at 6 elever svarer bekræftende på, at *de* har oplevet problemer med sikkerheden i den organisation, de er ansat i. Årsagen til dette kan måske findes i organisationens holdning til softwaresikkerhed, eftersom respondenterne for disse virksomheder angiver, at der ikke er fokus på softwaresikkerheden.

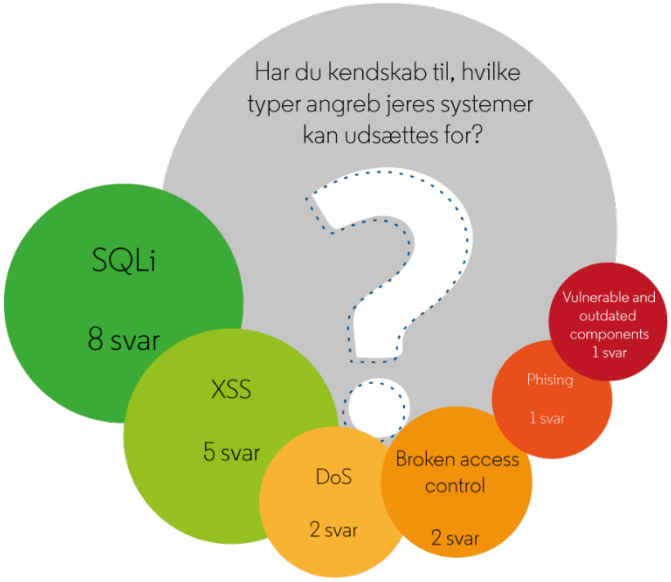


Figur 13: Sikkerhedsproblemer i organisationen

I forhold til spørgsmålet om, hvorvidt eleverne har kendskab til, hvilke typer af angreb deres systemer kan være udsat for, ligger der en udfordring i forholdet til tolkning af data. Spørgsmålet er, om deres svar bunder i, hvad *de ved om deres systemer i organisationen* eller om deres svar er afgivet ud fra *deres generelle kendskab til angrebstyper*. Noget i elevernes distancerede svar indikerer, at deres besvarelser læner sig mod det generelle kendskab - blandt andet udtaler en elev: *"…. så er der også noget som Social Engineering, med at få lokket dataene ud af folk ved at få dem til at skrive eller oplyse på anden måde*". Det er dog værd at nævne, at 4 elever ikke kan svare på spørgsmålet, hvilket kan indikere, at de forholder sig konkret til deres egne og organisationens systemer.

For at skabe et overblik over elevernes svar, har vi klassificeret deres svar i forskellige angrebstyper og sårbarheder. Ud fra elevernes svar virker det som om, de er bevidste om forskellige sårbarheder, når det kommer til virksomhedernes systemer. 8 nævner SQLi, som potentiel trussel og 5 nævner XSS. En elev nævner, at de i virksomheden har *outdated* komponenter, og han er opmærksom på den problemstilling. To elever nævner, *"broken access control"*, omend de ikke kan definere begrebet.

Det er værd at nævne, at flere elever nævner tid og opgaveprioritering som en faktor i forhold til det manglende sikkerhedsfokus. En elev udtaler: *"Det er altid noget bliver der bliver diskuteret, men det er ikke altid førsteprioritet"*



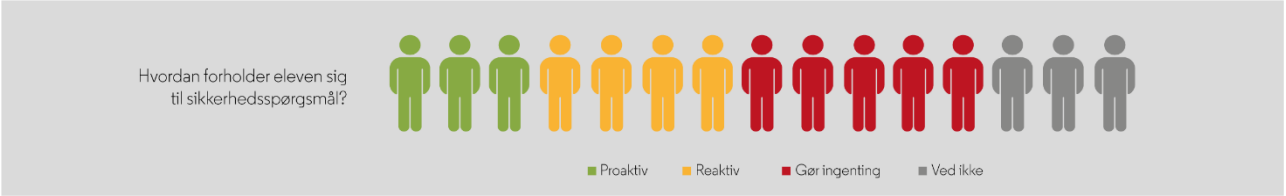
Figur 14: Angrebstyper og sårbarheder

Sikkerhedsambassadøren

Når vi vælger overskriften "Sikkerhedsambassadøren", gør vi det i afsæt i et ønske om, at vores elever skal være bannerfører i forhold til sikkerheden. For at det kan blive en realitet, kræver det en reel indsats fra eleverne selv. I denne kategori stilles eleverne to spørgsmål, som handler om egen indsatsen.

Til første spørgsmål: *"Hvor godt føler du dig klædt på, til at håndtere softwaresikkerhed?"*, svarer 4 ud af 15, at de føler sig *godt klædt på*, 6 svarer modsat og én kan ikke svare. Det er lidt interessant, at de 4 elever, som giver udtryk for, at de er godt rustet, faktisk ikke kan definere begrebet softwaresikkerhed. Den ene mener, at softwaresikkerhed handler om at kryptere data i databasen, en anden definerer softwaresikkerhed som: *"Sikkerhed for, at man skal sikre data…"*. Den 3. respondent svarer direkte på spørgsmålet: *" Jeg føler mig, jeg føler mig ret godt klædt på. Jeg har haft nogle ret tunge forløb med sikkerhed, hvor jeg synes vi har lært om de forskellige muligheder for brud"* og alligevel nævner denne respondent kun SQLi som mulig angrebstype til spørgsmål 4, og han ser datasikkerhed som værende noget med adgangskontrol, roller og rettigheder.

Til spørgsmålet om, hvad eleverne gør for at holde sig opdateret i forhold til sikkerhedsspørgsmål har vi kategoriseret svarene i segmenter. Eleven er *proaktiv*, altså opsøger selv sikkerhedsinformation. Eleven er *reaktiv*, han opsøger ikke selv information aktivt, men læser, hvis det er relevant. Derudover er er der to yderligere kategorier, eleven gør *ingenting* eller *kan ikke svare*.



Figur 15: Elevernes reaktion på sikkerhedsspørgsmål

De elever, som kategoriseres som proaktive, angiver, at de får deres viden gennem Reddit, Podcast og Center for cybersikkerhed. De reaktive elever får deres informationer serveret gennem nyhedsfeed og sociale medier og reagerer efterfølgende på indholdet, hvis det har interesse. En enkelt elev fortæller dog, at inden han skal i gang med et nyt projekt, så søger han lidt information om, hvordan andre har håndteret sikkerheden i lignende situationer.

Som tidligere nævnt ser det ud til, at det ingen betydning har, hvor langt i uddannelsesforløbet eleverne er i forhold til forståelsen af softwaresikkerheden. Der er ingen tydelige mønstre, som viser, at begrebsforståelse øges, eller at softwaresikkerheden fylder mere i takt med, at eleverne kommer længere frem i deres uddannelse.

Delkonklusion på vores undersøgelser

Generelt er eleverne meget konkrete i forhold til deres besvarelser. De har meget fokus på selve angrebstyperne og konkrete forsvarsmekanismer. De taler meget om kryptering og hashing, og det virker som om, at deres svar afgives ud fra en fælles referenceramme mod database og opbevaring af data.

Det er tydeligt at se, at begrebsdefinitionerne generelt halter bagud både i forhold til spørgsmål 1 og 10, men også i forbindelse med spørgsmål 7. Eleverne har svært ved at komme med klare definitioner på for eksempel *broken access control*. De kan sagtens redegøre for, at nogle får rettigheder og adgang til noget, de ikke skulle have haft, og det er noget skidt, men at sætte en klar definition – det kan de ikke. Så kan man diskutere, hvorvidt disse begrebsdefinitioner er relevante eller ej, når nu eleven *ved*, at der kan opstå et potentielt problem. Det kan dog være svært at søge og skaffe nødvendig og relevant viden gennem f.eks. OWASP, CVE'er[7] eller CWE'er[8], som klassificerer sårbarheder, svagheder og angreb i disse begrebsdefinitioner. Det kan måske også være en af årsagerne til, at eleverne ikke aktivt søger information på disse platforme, *fordi de ikke ved, hvad det er, de leder efter*?

Det er svært at konkludere noget i forhold til sikkerheden i virksomheden. Der er nogle tendenser som man kan stille sig undrende over, eksempelvis at der er flere elever, der nævner, at de har oplevet problemer med sikkerheden i organisationen, men samtidig fylder sikkerheden ikke meget i hverdagen i forhold til deres arbejde. Skyldes det mon ligegyldighed, risikovillighed eller manglende viden hos ledelsen eller generelt i organisationen? Det er svært at svare på, men ved at uddanne vores elever til sikkerhedsambassadører, kan eleven måske, i sin organisation, skabe mere fokus gennem dialog ved at kunne påpege direkte svagheder og sårbarheder i virksomhedens software. I forhold til spørgsmålet omkring kendskabet til angrebstyper, er det interessant at se, at eleverne stort set kun nævner elementer, som vi har gennemgået i undervisningen. Vi lever i en tid, hvor systemer udsættes for angreb hvert 39. sekund (Bulao, 2023) og alligevel nævner eleverne primært kun SQLi og XSS. Så noget tyder på, at eleverne på deres respektive arbejdspladser ikke arbejder særlig meget med

[7] https://cve.mitre.org/
[8] https://cwe.mitre.org/

softwaresikkerheden, som ellers er en del af praktikmålene, og som er en gensidig aftale med mellem skolerne, undervisningsministeriet og industriens uddannelser.

Hvis vi skal uddanne eleverne til sikkerhedsambassadører, skal eleverne være aktiv deltagende og lære at være mere proaktive i forhold til sikkerhedsspørgsmål - men hvordan? I dagligdagen refererer vi ofte til både OWASP og NIST som gode informationsbanker, og alligevel søger eleverne ikke informationen her. Vi ved fra erfaring, at eleverne generelt har *modstand* mod at læse eller i hvert fald reduceret læselyst. Vi har tidligere forsøgt at introduceret både CVE og CWE, men uden held. Der er for meget information, det er svært at navigere i, og de har svært ved at finde den bid af information, som de skal bruge, hvilket måske kan hænge sammen med de manglende begrebsdefinitioner.

Ser vi på elevernes egne forhold til, hvor godt de føler sig klædt på i forhold til softwaresikkerheden, er der en overvægt, der faktisk svarer, at det godt kunne være bedre. Det vidner om, at eleverne godt selv ved, at de har huller i deres sikkerhedsviden fremfor de elever, som mener at være godt klædt på. Det virker i hvert fald som om, der er en uoverensstemmelse mellem, hvordan de opfatter sig selv kontra, hvad de siger og gør. Det handler måske langt mere om, hvad elever ved og ikke ved, der er måske tale om en manifestation af dunning-kruger effekten? Hvis eleven f.eks. tror, at sikkerheden begrænser sig til emner som SQLi, Phishing, XSS og Social Engineering, så giver det måske mening, at de svarer som de gør. Var vi, f.eks. blevet stillet det samme spørgsmål for et par år siden, så havde vi nok svaret det samme. Nu ved vi af erfaring, at vi kun kender til toppen af isbjerget.

Læring

I en opgave som denne er det svært at komme uden om læringsteorien som et grundlæggende tema, både fordi det er en relativ vigtig del af vores hverdag som undervisere, men også fordi vi, gennem vores undervisning de seneste år, har set, hvor afgørende læringen er i forhold til elevernes opfattelse af softwaresikkerheden.

Hvornår kan man lære noget?

Som undervisere er vores fornemmeste opgave at facilitere læring hos eleven, hvorved han eller hun øger sin viden, færdigheder og kompetenceniveau.

En stor overvægt af de elever, som starter på vores uddannelse, hører til generation Z. De særlige kendetegn ved denne generation er, at de er digitale indfødte, de kan virke dovne, de multitasker eller skifter hele tiden fokus på forskellige opgaver, og de har løbende behov for at holde sig opdateret og stimuleret, hvilket gør, at deres koncentrationsniveau er *væsentligt* forringet i forhold til tidligere generationer (Rothman, 2016).

Hvad driver generation Z?

Drivkraften er, ifølge Illeris, en væsentlig faktor for at lære noget, men hvad driver egentligt et menneske? I følge Illeris består drivkraften af flere elementer, som omhandler individets psykiske energi som både motivation, følelser, nysgerrighed og ikke mindst vilje. Som undervisere har vi ikke meget indflydelse på den enkelte elevs drivkraftsdimension. Vi kan gennem ydre påvirkninger pege eleverne i en bestemt retning eller skabe rammerne omkring læringsrummet, men som udgangspunkt skal eksempelvis *viljen* til at lære noget komme inde fra eleven selv.

Drivkraften og motivationen hos generation Z stiller nogle udfordringer til de, der enten skal undervise eller lede dem. De er opvokset i en tid, hvor multitasking er mere reglen end undtagelsen, og deres motivation daler og stiger i takt med deres omgivelser og den kontekst de befinder sig i. Netop motivationen, eller mangel heraf, er en væsentlig faktor, når vi ser ind i erhvervsuddannelserne. Einer Skaalvik (Skaalvik, 2020) går endda et skridt videre og udtrykker, at vi står midt i en motivationskrise.

Årsagen herfor mener Skaalvik er, at eleverne aldrig får det, man i fagtermer kalder mestringsoplevelser – altså at de stilles konkrete opgaver som de kan løse, men som samtidig også kræver, at de skal anstrenge sig. En anden årsag til denne motivationskrise er, at eleverne skal kunne se relevans i de opgaver, de skal løse. Gert Bista (Bista, 2020) mener, at den manglende motivation hos de mange unge skal findes i meningsfuldhed. Opgaver, som ikke kan overføres til egen hverdag, og som samtidig opleves ikke værende værdifulde og nyttige, svækker elevernes motivation. Generation Z motiveres af at engagere sig med noget, de brænder for og helst gennem praktisk arbejde (*Learning by doing*). De bruger ofte humor som en måde at balancere mellem afslapning og seriøsitet. Det er en generation, som befinder sig bedst i en individualiseret læringsproces (Seemiller & Grace, 2018), hvorfra de kan opnå selvrealisering gennem personlige "*achivements*" og avancement til "*nye levels*" i deres eget tempo, og hvor resultatet af deres anstrengelse giver en øjeblikkelig feedback (mestringsmotivation). Feedback er ikke bare feedback. Denne generation er opvokset med konceptet "*likes*", hvilket betyder, at de som udgangspunkt forventer feedback tager udgangspunkt i det de gør godt (Marzullo, 2020). De trives godt og drives fremad i deres proces, når de opnår belønninger f.eks. i form af guldstjerner eller badges, som tildeles efter *veludført* arbejde. Selvom de fortrækker den individualiserede proces, betyder det ikke, at generationen er særlig konkurrence præget. Det er tværtom en generation, som er både hjælpsom og socialt fokuseret, men som ikke har brug for, hverken offentlig anerkendelse eller være i konkurrence med andre for at føle sig motiveret, det kan tværtimod have den modsatte effekt.

Humor kan have indflydelse på de emotionelle aspekter i forhold til drivkraften, men hvad mere interessant er, at hygge også er en væsentlig motivationsfaktor i forhold til drivkraften. Er omgivelserne hyggelige, har det indflydelse på elevernes følelser og ad den vej øges motivationen (Nieżurawska, Kycia, & Niemczynowicz , 2023).

Som nævnt er det ikke kun motivationen, som er drivkraften bag elevens læring, nysgerrighed kan også spille en væsentlig rolle. Ved at øge elevernes nysgerrighed, dannes der grobund til fordybelse i et eller flere ukendte områder, som eleven ønsker at udforske og øge sit kompetenceniveau og som er motivationsfremmende. Af natur er generation Z en relativ nysgerrig generation, som stiller sig selv og andre mange spørgsmål.

Indholdet i læringen

Drivkraften er ikke den eneste dimension, der har indflydelse på om læring finder sted. I tilegnelsesprocessen skal man, ifølge Illeris, også forholde sig til selve indholdet – altså det, der skal læres og på hvilket taksonomisk niveau noget skal læres. Begge dimensioner er indbyrdes afhængige og påvirker hinanden. Generation Z stiller andre og anderledes krav til, hvordan de som udgangspunkt vil have fagligt stof formidlet og præsenteret i forhold til tidligere generationer.

Den *"klassiske metode"*[9] at formidle læring på fungerer ikke for disse unge mennesker. Meget af den viden, vi tidligere har formidlet i klasserummet, har eleverne i dag selv mulighed for at indsamle gennem søgninger og digitaliserede platforme– nogle gange endda hurtigere end underviseren.

Generation Z har generelt en lavere koncentrationsevne (DTU, 2019) end tidligere generationer. Flere undersøgelser konkluderer, at det skyldes den teknologiske udvikling og den hastighed vi modtager information i. De konstante påvirkninger, som hjernen udsættes for, minder lidt om at poppe popcorn i mikroovnen (Cohen, 2011). Denne konstante belastning gør, at det er sværere for denne generation

[9] Tavle og forelæsningsmetodik

at koncentrere sig, og selve fordybelsesprocessen er afgørende for enten den assimilative eller akkomodative læring (Illeris, 2015 s.61-65).

Denne generation har fremdrift i deres læringsprocesser, når det, der skal læres, er både virkeligheds- og praksisnært, problemløsende, og de kan se formålet med at lære "*noget*" og at få fyldt deres værktøjskasse med brugbare redskaber til en fremtidig karriere. Allerhelst vil de selv have kontrol over, hvornår de skal lære "*noget*", hvor hurtigt det skal læres og i hvilket miljø de skal lære.

Som lærende i dag er der mange muligheder for at lære. Der stilles mange digitale platforme til rådighed, og der er en klar tendens til, at den fysiske verden flytter ind i mere digitaliserede former. Teknologien gør det muligt at kombinere materialer og deres modalitet i forhold til undervisningen, som gør, at elever i dag forventer en flerdimensionel adgang til information som for eksempel gennem læringsplatforme, hvor tekst, lyd, billeder, videoer og andet interaktiv materiale kombineres.

Generation Z er langt mere visuelt orienteret end tidligere generationer og med de digitale muligheder, som i dag er til rådighed, er YouTube blevet én af deres fortrukne læringsplatforme. Når de foretrækker videomediet fremfor tekst, skyldes det muligvis, at hjernen kan processere den visuelle information 60.000 gange hurtigere (Slade-Silovic, 2018) end den skrevne. Det kan virke appellerende til denne generation, netop fordi det ikke kræver så meget anstrengelse og fordybelse. Ser man på de "*unges*" læselyst, er den i kraftigt fald. Ifølge *Center for anvendt skoleforskning* mister især drenge lysten til at læse, og det er faktisk kun hver anden dreng, som i 15-årsalderen har lyst til at læse (Rymann, u.d.) – og vi har en nagende mistanke om, at han havner på gymnasiet, fremfor erhvervsskolen. Vi bemærker også den manglende gejst i forhold til læsning i hverdagen. Det er svært at få eleverne til at læse eksempelvis den officielle dokumentation fra Microsoft i forhold til en konkret klasse eller metode. I stedet anvender de hellere *stack overflow,* finder noget kode og stiller sig tilfredse med det, uden at forstå, hvordan det fungerer. Dette udsagn underbygges også af en undersøgelse vedrørende de unges digitale undersøgelsesvaner (Purcell, et al., 2012) . Der er sket et paradigmeskift fra at være nysgerrige og undersøgende omkring et emne, handler det nu mere om at finde svarene eller løsningen for at komme videre til næste opgave.

Samtidig kan videoer være med til at fastholde koncentrationen og øge engagementet hos eleverne i og med, at der hele tiden opstår tilstandsskifter i form af billeder og lyd. Video er dog ikke bare video. Skal man fange denne unge generations opmærksomhed, er det vigtigt at undgå forelæsningssituationer, de betragtes som kedelig og uinspirerende. Vi har derfor taget udgangspunkt i konceptet "*flipped classroom*" og de anbefalinger, der gives i forhold til videodesign. Videoerne må ikke være for lange, faktisk anbefales det, at en video ikke er længere end 7 minutter og at indholdet i videoen begrænses til kun at indeholde et enkelt emne (Wong, 2022). Når der arbejdes med videomateriale, er der to kommunikationskanaler, den ene bruges til visuel kommunikation og den anden til audio. Disse to elementer er indbyrdes afhængige, videoen kan være flot udformet, men speakeren opfattes som tør og kedelig eller vice versa. Opfatter eleven indholdet som værende kedeligt, er der relativ stor sandsynlighed for, at eleven bare ser videoen, fordi han *skal,* men ikke ser den som relevant eller, at han er videre til en anden opgave. Det er her vigtigt at have i mente, at den yngre generation, i forhold til digitale medier, har en koncentrationsevne helt nede på omkring 8 sekunder, hvilket faktisk hævdes er mindre end en guldfisk – den har 9 (Consumer Insights, Microsoft Canada, 2015). Generation Z's læring afhænger i stor grad af dem, der skal "*undervise*" dem. Ved at underviseren eller facilitatoren er motiveret og engageret, pirker det til elevernes nysgerrighed og interesse (Seemiller & Grace, 2018). Engagementet og entusiasmen skal i forholdet til videomateriale altså findes både i det visuelle udtryk og i intonationen hos speakeren.

Kønnet har også en afgørende betydning for, hvordan denne generation lærer. Drenge er tilbøjelige til at fortrække en mere logisk form for læringsstil (Seemiller & Grace, 2016). En logisk læringsmetode tager afsæt i at den lærende er metodisk og lineær tænkende. De fortrækker at være organiseret, systematiske og nedbryder opgaver. De er resultat- og detaljeorienteret, arbejder bedst ud fra et problem som skal løses, de tager beslutninger baseret på fakta eksempelvis i form af statistikker (Time 4 learning, u.d.). De fungerer ikke særlig godt med vage instruktioner, og det skal fremgå meget tydeligt *"hvad det er de skal"*. Logiske lærende trives særlig godt med at løse gåder, hvor de selv skal finde løsningen (Homeschool blog, 2022).
Indholdet dækker, som nævnt, både over det, der skal læres og hvilke niveauer noget skal læres på. Indenfor erhvervsskole regi arbejder man med 2 typer af mål. Det ene er uddannelsesmål, og det andet er kompetencemål. Uddannelsesmålene angives i den pågældende fagretnings uddannelsesordning, hvor uddannelsesmålene er grupperet og placeret i en række fagpakker. Kompetencemålene er derimod angivet i bekendtgørelsen for uddannelsen. Det eneste overordnede kompetencemål, som omhandler sikkerhed i bekendtgørelsen for data- og kommunikationsuddannelse, er som følger:

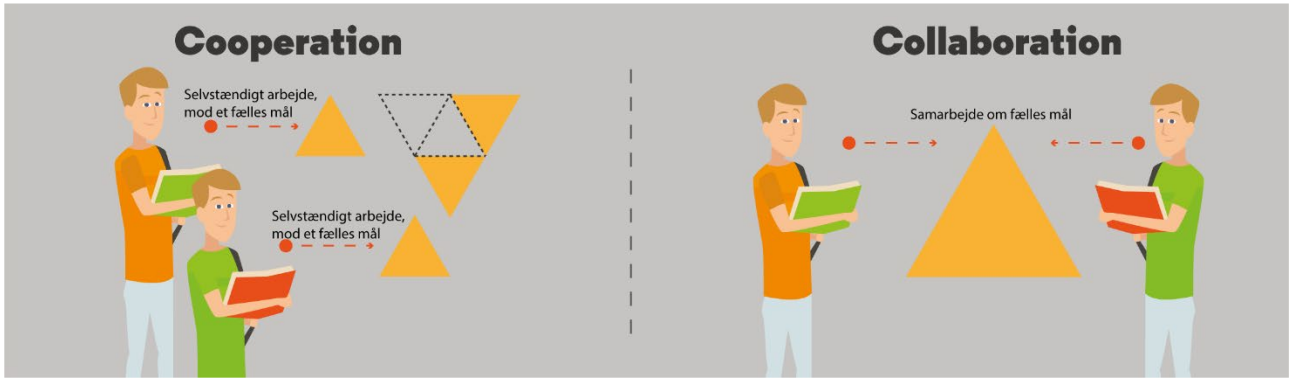
Lærlingen kan designe, planlægge og udvikle programmer, som gør brug af et udviklingssprogs tilknyttede sikkerhedsværktøjer, og kan endvidere udvikle programløsninger, som indeholder de fornødne sikkerhedsløsninger i forhold til en given opgave. (Retsinformation, 2023, §4, stk. 32)

Det springende punkt er ordet "*fornødne*", altså om det skønnes nødvendigt. For at kunne implementere de "*fornødne*" sikkerhedsforanstaltninger, er det altså ikke nok for eleverne at kende til f.eks. injektionsangreb, de skal også kende til forsvarsmekanismer og hvordan disse kan implementeres i den aktuelle kontekst.

Alt der udenom…

Samspillet til omverdenen har også en betydning for elevernes læring på flere fronter. Nogle gange styres læring af den indre motivation hos eleven, lysten til at lære nyt – andre gange ledes vi hen mod ny læring gennem sociale fællesskaber og samarbejde.

Generation Z er af natur meget sociale og har store kontaktflader, men når det kommer til læring, fortrækker størstedelen at arbejde alene fremfor gruppearbejde. Tvinges de i gruppearbejde, skal det helst foregå i små grupper, hvilket går godt i tråd med deres drivkraft, nemlig det at de allerhelst selv vil bestemme tempo og omgivelser. Selvom man kan opfatte denne generation som selvcentreret og individualister, så er der mere end øjet kan se. Faktisk foretrækker eleverne at lære i fællesskab, men mere som parallel læring. På engelsk findes der to gode ord, til at beskrive denne situation, *cooperation* og *collaboration* (dansk: samarbejde).

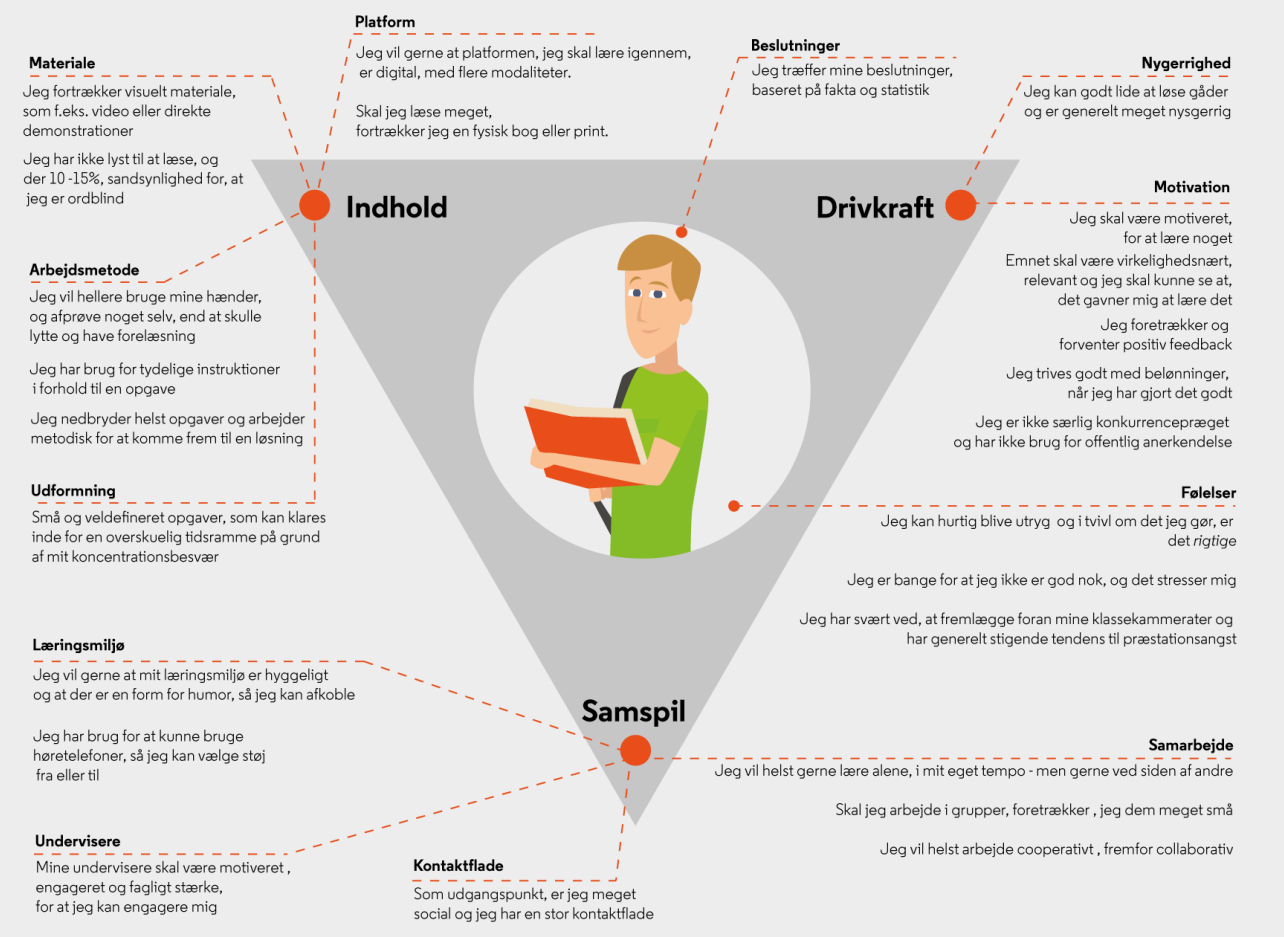


Figur 16: Cooperation og collaboration

Forskellen mellem *cooperation* og *collaboration* er den tilgang eleverne har til samarbejdet. Ved *collaboration* samarbejder eleverne om et fælles mål og er indbyrdes afhængige af hinanden, hvorimod cooperation handler om, at eleverne har forskellige mål, men at man støtter hinanden fremad i læringsprocessen, noget kunne tyde på, at generation Z fortrækker dette samspil, fremfor *collaboration*. Udover at undervisningsmiljøet skal være hyggeligt og rart, er det vigtigt for Z'erne, at der er fred og ro i forhold til deres læreproces. Flere vælger at iføre sig hovedtelefoner, hvorfra de kan lytte til musik eller "*white noise*", men det er vigtigt for dem at være i nærheden af hinanden og hoppe ind og ud af fællesskabet efter behov.
De ydre omgivelser har stor betydning i forhold til disse elevers trivsel. Der er desværre en stigende tendens til stress og præstationsangst og generel mistrivsel hos denne uge generation (Børns vilkår, 2022), som er med til at sætte benspænd for læring i de sociale relationer. Eleverne bliver ofte usikre på om de gør det rigtige og har løbende behov for bekræftelse, hvilket også besværliggøre gruppearbejde. Frygten for fiasko er desværre fremherskende i uddannelsessystemet, og der er mange unge mennesker, som i dag har store vanskeligheder og som er angste for at begå fejl og ikke præstere "*godt nok*". Det er derfor ekstremt vigtigt at tænke samspilsprocessen og undervisningsklimaet ind i forholdet til elevernes læring og deres motivation. Carolyn Jackson (Jackson, 2020) anbefaler, at uddannelsesklimaet skal ændres fra at handle om præstationer til i stedet at give eleverne trygge rammer til at turde eksperimentere og fejle.

Elev Z

På baggrund af, hvad vi ved fra egen empiri og det forskningen fortæller os, både i forhold til læring og generation Z, er det lidt som at åbne Pandoras æske. Vi har forsøgt at kortlægge Illeris læringstrekant, sammen med en generalisering af den typiske generation Z datateknikerelev.



Figur 17: Kortlægning af generation Z i forhold til Illeris læringstrekant

Vi tænker, at vi altså skal finde en digital løsning, hvor eleverne kan lære om sikkerhed i software i deres eget tempo uden at skulle konkurrere med andre, helst i valgfrie og rolige omgivelser, men gerne sammen med andre. Der må ikke være meget tekst, som skal læses, og indholdet skal helst være visuelt, gådefuldt, faktabaseret, meningsfyldt og virkelighedsnært med et gran humor. Der skal tages udgangspunkt i konceptet *"hands-on"*, hvor løsningen ikke ligger lige til højrebenet og som kræver aktiv deltagelse, men uden at opgaven bliver for stor og utydelig. Løsningen skal ydermere understøtte muligheder for positiv feedback, åbning af nye "*levels*" og kvittere med belønninger.

Som undervisere er fristelsen stor til at starte et sikkerhedsemne med den teoretiske viden og abstrakte modeller og derefter bevæge sig ned mod en mere praktisk anvendelse. I de seneste par år har FIT-modellen været flittigt brugt i vores undervisning om sikkerhed. Imidlertid viser resultaterne af undersøgelsen, måske ikke overraskende, at eleverne ikke har taget begreberne til sig i det omfang, vi nok havde forventet. Selvom integritetsbegrebet udgør halvdelen af undervisningen i en uges

databaseundervisning på elevernes andet hovedforløb, kan 60% af de adspurgte elever ikke definere begrebet, og kun tre elever har et tøvende bud på en definition. Dette rejser spørgsmålet om relevansen af, og om det overhovedet kan *betale* sig, at undervise i modellen. Skal man analysere lidt på egen praksis – og det skal man, så giver det hele måske mening i forhold til elevernes "manglende" begrebsforståelse. Måske har eleverne svært ved at se relevansen af og hvordan de aktivt kan bruge FIT modellen som en del af deres hverdag. Derfor er det interessant at finde andre og måske mere effektive undervisningsmetoder, som kan sikre, at eleverne forstår og kan anvende sikkerhedskoncepter og begreber og ad den vej udvikle sikre softwareløsninger

Vi foreslår i stedet en *bottom-up* tilgang, hvor eleverne starter med konkrete angreb og sårbarheder, og udvikler deres praktiske færdigheder til for eksempel at identificere sårbarheder og udvikle passende sikkerhedsforanstaltninger gennem forståelse af angrebsvektorer. Vi har, på tidligere undervisningsforløb, set, at eleverne er meget begejstrede når emnerne omhandler konkrete angrebstyper. Vi håber ved at starte nedefra og lade eleverne "*hacke*" konkrete systemer, at deres motivation for softwaresikkerheden øges. Vores håb er, at de bliver så nysgerrige og engagerede, at de selv fremadrettet vil opsøge relevant information samtidig med, at de får udviklet deres praktiske færdigheder i kombination med teori og koncepter, som kan forberede dem på de udfordringer, de vil møde i den virkelige verden.

Mission Possible

Med afsæt i vores elever, deres vilje og motivation og ikke mindst evner i kombination med ZBC's didaktiske grundlag er vi kommet frem til at forsøge at introducere softwaresikkerheden gennem *gamification*. Vi har derfor udviklet en web-platform og et "*laboratorie*[10]", hvorfra eleverne kan arbejde med softwaresikkerheden i praksis, eksempelvis gennem hacking og udnyttelser af sårbarheder, helt i deres eget tempo.

Platformen indeholder mange af de elementer, som eleverne efterspørger i forhold til læring. De primære materiale er udarbejdet gennem videomedie, og det er begrænset med tekst, som skal læses. Opgaverne er gådefulde, men samtidig er de tydelige og afgrænsede, som eleverne får point for ved gennemførelse.

[10] Opsætning af fysisk udstyr med servere og netværk

Figur18: Mission Possible

Ideen til denne platform udspringer af vores egne erfaringer og observationer, som vi har gjort i klasselokalet. Som en del af fagpakken softwaresikkerhed på Aalborg universitet stiftede vi bekendtskab med Hauukins platformen, som er en træningsplatform til cyber security (Institut for Elektroniske Systemer, u.d.). Konceptet bag platformen er brillant, her får man en kæmpe legeplads stillet til rådighed. Problemet er bare, at hvis man ikke ved, hvordan man gynger, så kan platformen virke både tung og svær at komme i gang med, og der er meget lidt hjælp at hente. Vi oplevede hurtigt, at vi selv gik i stå og mistede motivationen, også selvom opgaverne var spændende og udfordrende. Denne oplevelse har vi bragt med til vores egen platform. Vi har derfor kaldt vores platform *Mission Possible*, vi vil gerne, at eleverne får en mestringsoplevelse, jf. Skaalvik og kan gennemføre. Når vi samtidig vælger at lave en platform, hvor elever kan "*hacke*", så skyldes det elevernes engagement. Når vi, i de seneste par år, har givet eleverne adgang til *Weapons4U,* har vi oplevet at eleverne har arbejdet meget koncentreret og målrettet med materialet og udtrykt stor begejstring.

Platformen giver eleverne mulighed for at oprette en profil, logge ind i systemet og gå i gang med en mission, som er niveaumæssigt svarende til det hovedforløb, de er tilmeldt. Overordnet set er platformen designet specielt til elevernes behov og deres forudsætninger, som danner grundlag for den didaktiske planlægning. Eksempelvis skal de ikke foretage SQLi angreb førend, de har haft undervisning i database og databaseservere.

Mission Possible er designet til at kunne tilføre flere missioner. En mission består af en række semi-selvstændige opgaver, hvor strukturen kræver, at eleverne løser én opgave, førend de kan starte på den næste.

Figur 19: Oversigt over Mission Possible

Som undervisere har vi fuld kontrol over hele platformen, hvilket er en enorm fordel i forhold til eksempelvis Hauukins. Det betyder, at vi løbende kan tilføje nye og relevante missioner i takt med ændringer i uddannelsesordningen eller andre emner, som vi finder relevante. Samtidig giver det også os, som undervisere, mulighed for at overvåge elevernes fremskridt og tilbyde støtte, når det er nødvendigt.

Det overordnede formål med hele platformen er at give eleverne mulighed for at lære noget omkring softwaresikkerhed gennem praktisk arbejde i et sikkert og kontrolleret miljø, hvor de både kan udforske forskellige scenarier og lære af deres fejl uden at forårsage skade på andre systemer. Vi håber, at eleverne kan trække deres viden og angrebsteknikker med *hjem* til deres praktiksted og der måske gennem samme eller lignende angrebsvinkel, kan højne virksomhedens softwaresikkerhed.

Vi balancerer på en meget skarp knivsæg. Vi er helt bevidste om, at vores beslutning om udvikling af denne platform har en skyggeside i form af etik. For er det egentlig etisk forsvarligt at lære eleverne, hvordan man for eksempel "*cracker*" password på en ZIP fil? Vores umiddelbare svar er ja, for hvis man ikke ved at beskyttelse af en ZIP fil kan crackes på mindre end 5-10 minutter, så ændrer man jo ikke sikkerhedspraksis. Eleverne bliver informeret om lovgivningen indenfor hacking og cyberkriminalitet, og det understreges tydeligt, at det, de foretager sig på *Mission Possible,* ikke er tilladt andre steder, og at det kan være ulovligt og kan have alvorlige konsekvenser.

Design af platformen

I forhold til platformens udformning og design, har vi taget udgangspunkt Burkes model (Burke, 2016, s.12). Vi har dog valgt at justere lidt på titlerne for de enkelte delprocesser, så de giver mere mening i forhold til vores løsning, men grundelementerne, fra Burkes model, er de samme.

Definer mål og succeskriterier

Vores overordnede formål er at give eleverne en "sikker" platform, hvor der er plads til at udfolde sig uden, at der kan opstå uheldige situationer, hvor eleverne får "angrebet" de forkerte med konsekvenser til følge.

Mere detaljeret ønsker vi også at:

- Eleverne bliver mere opmærksomme på sikkerhedsaspekter
- Eleverne kan se, hvor nemt det kan være at udnytte sikkerhedshuller
- Eleverne kan få værktøjer til at forebygge potentielle trusler i forhold til deres egne software implementeringer
- Elever påbegynder en begrebsdannelsesrejse i forhold til softwaresikkerheden

Burke understreger, at målene, udover at være realistiske, opnåelige og tydelige, også skal opstilles så succeskriterierne er målbare – men hvordan måler man holdninger? Sikkerhedsimplementeringer handler i stor grad om holdninger og risikovillighed. Vi kan sagtens opstille konkrete mål, som f.eks. at 95% eleverne kan oprette et mere kompleks password eller at 90% af vores elever implementerer SQL parameteriset forespørgsler gennem *stored procedures*, men i bund og grund er det ikke det, vi forsøger at opnå. Det, vi ønsker, er en holdning- og adfærdsændring hos eleverne, så de, i deres hverdag, træffer beslutninger i forhold til deres softwareimplementeringer på baggrund af sikkerhedskonteksten. Den effekt kan være svær at måle over en kort distance, men skal ses i en bredere forstand i forhold til uddannelsens længde, Det betyder, at vi reelt først på sidste hovedforløb, elevernes svendeprøve, kan se effekten af både vores og deres anstrengelser. Der kan dog være indikationer undervejs, som peger på, om eleverne er på vej i den rigtige retning.

Deltagerfeltet

Burke understreger, at det er ekstremt vigtigt at have en dyb forståelse af deltagerne, hvis de følelsesmæssigt skal kunne engagere sig. Det går godt i spænd med, at enhver didaktisk beslutning, i erhvervsskolen, som oftest tager udgangspunkt i elevernes forudsætninger. Disse forudsætninger kan være både af faglig, social, fysisk og psykisk karakter (Hiim & Hippe, 1999). Vi har som udgangspunkt valgt at designe vores platform ud fra disse kriterier ved at gøre det muligt at opdele "*gameplay*" i flere separate spil med enkeltstående udfordringer. Disse baseres primært på elevernes faglige forudsætninger i kombination med den fagrække de møder på deres indeværende hovedforløb, så der opstår en naturlig progression.

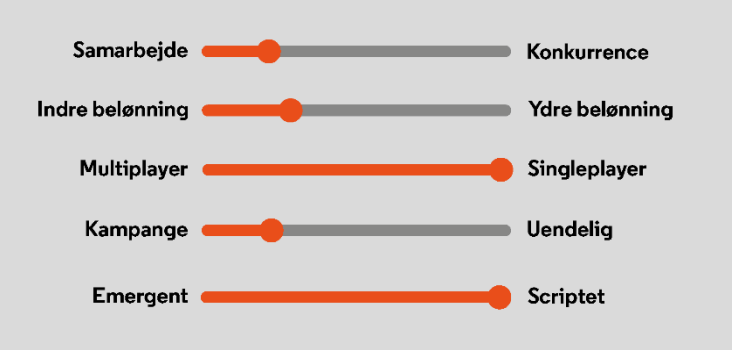
Det er vigtigt at understrege, at vi ønsker at denne platform skal være på frivillig basis for eleverne og drives gennem lyst til at lære og være med. Ingen elever skal hverken føle sig tvunget eller "udstødt", fordi de ikke ønsker at deltage.

Deltagernes mål

Der skal, ifølge Burke, være en række deltagermål, som i et eller andet omfang som regel overlapper det generelle formål, men ikke altid, og sådan er det som regel også indenfor undervisningssektoren. Vi har som underviser ofte et overordnet, og til tider et skjult, mål i forhold til elevernes læring, hvorimod eleverne er meget konkrete og drevet af en færdighed. Vores mål og elevernes mål på denne platform er ikke direkte forbundet, men i det brede perspektiv er de samstemmende. Vores mål henleder på adfærd og holdninger, hvorimod elevernes mål er langt mere konkrete. Hvilke mål, som elever skal opfylde, afhænger af hvilken mission de påbegynder. Som vi påtænker at designe platformen, skal der være en overordnet mission for hvert hovedforløb, og målene er derfor ikke generiske, men placeres under hver mission.

Find motivationen

Dette emne handler om selve strukturen for selve spillet, altså hvordan tænker vi, at eleverne skal arbejde med platformen. Skal de for eksempel samarbejde eller konkurrere mod hinanden? Burke anbefaler, at man tager udgangspunkt i 5 overordnede parametre, som man kan skrue på, og de har alle betydning for, hvordan eleverne motiveret arbejder med materialet.



Figur 20: De 5 parametre

Samarbejde eller konkurrence?

Som udgangspunkt ønsker vi ikke, at platformen skal danne grundlag for en stor konkurrence. Når vi ser på, hvad der motiverer vores elever, så kan indførelse af et stærkt konkurrenceelement have den modsatte effekt. Elever, som muligvis ikke er så fagligt stærke, kan risikere at vælge spillet og platformen fra for ikke at virke "*dum*" og tabe ansigt i forhold til deres holdkammerater. Samtidig kan konkurrenceelementet også give andre blod på tanden til at fortsætte. Vi vil derfor give mulighed for, at eleverne i spillet kan gøre deres profil *public*. En offentlig profil giver mulighed for at se andre offentlige deltageres progression og belønninger gennem et *scoreboard*. Eleverne må meget gerne samarbejde og hjælpe hinanden videre i processen, dette kan bidrage til at opbygge positive relationer og øge deres følelse af tilhørsforhold i et motiverende socialt fællesskab.

Indre eller ydre belønning?

Motivationen spiller en afgørende betydning i forhold til spillets udformning. Et belønningssystem kan have en motiverende effekt afhængig af, hvordan den udformes. Ser vi på uddannelsessystemet har vi ikke mange muligheder for at tilbyde nogle former for belønninger til eleverne, som kan motivere dem fremad i processen. Den eneste form for belønning, vi kan tilbyde, er karakter efter hvert fag holdt op mod de faglige mål. Vi ønsker dog ikke en præstationsfremmende platform, og derfor vælger vi at fjerne "karakterræset" fra platformen, og den indgår derfor ikke i elevernes summative evaluering. Det går godt i tråd med Alfie Kohn's udsagn: *"Extrinsic motivators (rewards) tend to reduce intrinsic motivation (people's interest in, or commitment to, what they're doing)"* (Bakar, 2022). Vi ønsker at eleverne lærer noget og ikke bare ræser igennem for at komme først. Samtidig trives de unge også med en form for belønning, så det handler om at finde balancepunktet. Vi vælger derfor at implementere et point system som motivationsfaktor.

Multiplayer / Solitary

Vores platform baseres på, at eleverne arbejder individuelt med opgaverne, som de tilsyneladende fortrækker det. De kan sagtens vælge at hjælpe hinanden, men selve platformen lægger an til individuel interaktion. Vi ønsker, at eleverne, selv udfører angrebene, så det ikke bare bliver en teoretisk gennemførelse, men derimod stimulerer deres haptiske hukommelse.

Kampagne/ Uendelig

Burke skelner mellem at udforme reelle kampagner eller udforme en løsning, som kører i det uendelige. Hvilket valg man træffer baseres på de mål, som er tilknyttet. Burke fremhæver forskellen ved at sige: *"Learning is endless, but training a specific skill are campaign"* (Burke, 2016). Den måde, vi har valgt at opdele vores setup, læner sig i stor grad op ad kampagnestrategien.

Emergent / Scripted
En platform, som den vi har tænkt os at implementere, kræver meget arbejde, hvis vi ikke styrer slagets gang. Ved en mere emergent løsning, kender vi ikke nødvendigvis resultatet af forløbet, den egner sig bedre til innovative processer. Vi har derfor valgt at låse os meget fast i en styrende retning i form af manuskripter for hver opgave, som ligger placeret i missionerne.

Spillets økonomi
Spillets økonomi spiller en central rolle i forhold til gamification konceptet. Økonomi refererer til den virtuelle økonomi, der kan eksistere på en gamification platform. Her kan spillere tjene eller købe virtuelle varer eller belønninger for at forbedre deres spiloplevelse eller nå bestemte mål. Burke beskriver, hvordan elementer som point, belønninger, ekstra power og badges, top-lister kan anvendes til at motivere og engagere brugere i spillet. Burke understreger vigtigheden af at designe en form for spil økonomi, der balancerer belønninger og udfordringer, så brugerne føler sig motiverede til at fortsætte med at spille eller interagere med platformen. Denne balance mellem forskellige elementer i en spiløkonomi, vil medvirke til, at brugerne føler sig motiverede både på kort og lang sigt.

Vi vil indføre to tiltag i forhold til spiløkonomien. Den ene er point og den anden et "*leader board*". Det højeste antal point, en spiller kan opnå for hver opgave inde i en mission, er 100. 100 point gives for at løse opgaven inden for bestemt tidsramme, det afhænger af opgavens sværhedsgrad samtidig med, at deltageren ikke gør brug af *hints*.

- For hver dag der går, hvor spilleren ikke har løst opgaven, fratrækkes 4 point
- For hvert praj, spilleren åbner, fratrækkes 10
- Der gives 4 stjerner for point mellem 91 og 100
- Der gives 3 stjerner for point mellem 75 og til 90
- Der gives 2 stjerner for point fra 50 og til 74
- Herefter gives 1 stjerne, så det laveste antal point, som gives, er altså 50

Der gives som også minimum 1 stjerne i forhold til elevernes forventning om positiv feedback.

"*Leader boardet*" er for de elever, som synes det er sjovt at konkurrere med andre. Eleverne vælger selv om deres profil skal være offentlig eller ej. Vælger de den offentlige profil, kan de løbende følge med i andre offentlige profilers progression og point for samme mission.

Spil og test – og gør det igen
Det sidste trin i gamification-processen er "*Play Test and Iterate*". Dette trin indebærer afprøvning og evaluering af gamification-løsningen for at identificere dens effektivitet og eventuelle områder, der kræver forbedring. Burke pointerer vigtigheden af at involvere brugerne i evalueringen og tage hensyn til deres feedback og holdninger.

Burke foreslår forskellige metoder til afprøvning og evaluering af gamification-løsningen, såsom beta-test, spørgeskemaundersøgelser og fokusgrupper. Det er afgørende at være opmærksom på de data, der indsamles under testene og bruge dem til at justere og forbedre løsningen. Ved at tage hensyn til feedback fra brugerne, og foretage løbende justeringer, kan gamification løsningen optimeres og forbedres for at opnå de ønskede resultater.

Missionerne
Som udgangspunkt kræver et spil et godt design. Et godt design kræver, at deltagerne synes, det er spændende at deltage, og at der er *"noget på spil"*. Med udgangspunkt i elevernes interesse og

motivation for læring har vi haft fokus på at reducere mængden af tekst, der skal læses, til et minimum. Vi gør brug af video som præsentations- og informationsmedie med både relevante og tidssvarende emner. Vi pirker til elevernes nysgerrighed og krydrer alle disse ingredienser med en knivspids humor.

Som tidligere nævnt har vi valgt at udforme designet i missioner, som består af en række sekventielle opgaver, der skal løses undervejs. Alle opgaver afsluttes med, at eleverne skal angive en nøgle, som de finder undervejs i deres bestræbelser for at låse op for næste opgave. Opgaverne i en mission er selvstændige og delvis uafhængige af hinanden.

For at bevare elevernes motivation, selvstændighed og give dem hjælp undervejs i processen, så de ikke går i stå, er der tilknyttet et eller flere *hints* til en opgave. En ledetråd indeholder en smule mere information, som gerne skulle guide eleven videre i forhold til deres konkrete opgave.

En ledetråd skal aktivt låses op af eleven og er designet til at blive brugt, hvis eleven er gået i stå og ikke længere ved, hvilken retning han eller hun skal gå. For hver gang eleven låser op for et *hint*, reduceres det summative antal point eleven kan opnå for opgaven. De enkelte ledetråde skal ikke have indbyrdes relation.

Mød Fred og Wilma, samt agenterne X og Y

Vi ønsker, at eleven skal føle sig som en del af et større og hemmeligt agentnetværk, og han eller hun er udstyret med særlige superkræfter i form af logik og nysgerrighed. Missionerne er opbygget ud fra en spændende historiefortælling, som hele tiden udfordrer eleven i at komme i mål for at redde verdenen mod de slemme banditter. Hver opgave stilles af agenterne X og Y gennem animeret video, som giver eleven introduktion til selve opgaven og eventuelle tips til at komme i gang. Agenterne er dog meget påpasselige med ikke at give en direkte indikation til, hvordan opgaven skal løse – det er altså lidt som at få stillet en gåde, hvilket bør appellere til vores elevtype. Når eleven efterfølgende har fuldført opgaven og afgivet nøglen, møder han Fred og Wilma. Fred og Wilma er to animerede karakterer forklædt som "*faglærere*". De giver eleven opfølgning og feedback på opgaven i form af refleksion til for eksempel, hvordan et angreb kan lade sig gøre eller en kort teoretisk gennemgang af et emne. Udover videomaterialet er der også en smule feedbacktekst, som enten understøtter videoen eller giver yderligere information.

Figur 21: Opgave flow

Maris Wilton

Som *proof of concept* har vi derfor designet vores første mission, som skal afvikles på platformen. Målgruppen er nye elever, som lige er startet. Vores udgangspunkt er, at sikkerhedspraksisser ikke er noget man lærer på en uge eller to. Det skal ind med modermælken, populært sagt. Vi håber, at vi allerede på første hovedforløb kan flytte elevernes *"mindset"* ved at udarbejde en mission, som fokuserer på gode softwareprincipper og simple angreb og som efterfølgende skal give eleverne nok viden og erfaring til at standse op og revurdere deres egen sikkerhedspraksis. Helt konkret ønsker vi, gennem denne mission, at eleverne bliver udfordret i forhold til deres eksisterende sikkerhedsviden. Eksempelvis tror en del af vores elever, at det er tegnsættets størrelse, som er afgørende i forhold til passworddesigns og flere tror, at man sagtens kan undgå *brute force* angreb.

Vi bliver meget udfordret i forhold til elevernes kompetenceniveau. Elever, som møder på deres første hovedforløb, har meget lidt eller ingen programmeringserfaring. De 10 uger, hvor de er på skole, bruges derfor på at undervise i grundlæggende programmeringsparadigmer og basal serverteknologi.

Figur 22: Fag og emner på første hovedforløb

Alle opgaverne tager udgangspunkt i emner, som eleverne har lidt kendskab til enten fra deres grundforløb eller som en del af deres første hovedforløb. Som resultat af dette kan de enkelte opgaver virke søgte og meget begrænset i deres udformning, men de er baseret på, at eleverne lykkedes med deres mission.

Målet for vores første mission:

- At eleverne kan se, hvor nemt det er at foretage *brute force* angreb
- Øge deres opmærksomhed i forhold til *Social Engineering*
- Forståelse for passwordkompleksitet
- At lære at holde hemmeligheder hemmelige
- Få kendskab til kryptering
- Opmærksomhed i forhold til princippet om "*Fail securely*"
- At få viden om angrebsoverfladen

Selve historien, for den første mission, tager udgangspunkt i kendissen Maris Wilton. Hun har fået kidnappet sin hund, og det er af allerstørste betydning at få fundet hunden i tide, især fordi den bærer på et meget dyrt diamanthalsbånd.

Figur 23: Opgaver til Missionen Maris Wilton

Historien starter med en introduktion til, hvad der er sket med Maris' hund, og hvordan kidnapperne er kravlet ud ad vinduet og ned af nedløbsrørene. Denne historie bærer alle opgaver i missionen med sig rundt, og banditterne bliver ikke fanget lige med det første, der opstår selvfølgelig nogle benspænd undervejs, som eleverne skal løse i de efterfølgende opgaver.

May the brute force be with you

... kidnapperne er stukket af med hunden, men de har tabt deres telefon....

At få fat i nøglen til paradiset afhænger af, hvorvidt en angriber er i stand til at skaffe sig adgang til himmeriget. En af de typiske måder, for angribere, at opnå adgang på, er at udføre et brute force angreb. Denne type angreb er relative simple og nemme at udføre, og angriberen vil altid på et eller andet tidspunkt opnå succes – det hele afhænger bare af tiden. En angriber kan let udvikle en simpel applikation, eller alternativt benytte allerede udviklet program til udførelse af et brute force angreb.

Eleverne har viden om brute force angreb på deres første hovedforløb – men stort set ingen har praktisk erfaring med den konkrete udførelse. Så første opgave i Maris Wilton scenariet er at "*cracke*" en virtuel mobiltelefon og skaffe pinkoden til at låse den op. Selve opgaven er ret enkel, der er tale om 4 cifre – som også er nøglen til at låse op for næste opgave. Når opgaven tager udgangspunkt i pinkoder, er der flere årsager til dette. For det første er det relativt simpelt at "*cracke*" en 4 cifret pinkode og derved håber vi, at eleverne får en mestringsoplevelse samtidig med at de får blod på tanden til at fortsætte med de efterfølgende opgaver i missionen. Den anden, og absolut vigtigere grund, er at give eleverne en generel viden om brugen af pinkoder – set ud fra et dannende perspektiv. Noget kan indikere, at pinkoder er på vej mod en renæssance. Microsoft har for eksempel indført pinkoder til deres desktop versioner og apps på mobiltelefoner afkræver også pin som en ekstra verifikation. For det tredje er det vigtigt for eleverne at erfare, at ondsindet kodeskrivning kan være programmering på begynderniveau. Selve mobiltelefonen er en simple eksekverbar fil, som har mulighed for at en pinkode med som argument. Vi forestiller os, at eleverne selv skriver et script, som

kaldes *exe* filen. De erfaringer som eleverne forhåbentlig vil drage sig, skal hjælpe med at forstå, at det teoretisk set er muligt for en angriber at bryde enhver kombination gennem et brute force angreb og at "*size does matter*". Som en del af *"undervisningsvideoen"* introduceres eleverne til implementering af simple forsvarsmekanismer f.eks. låsning af antal forsøg og logning.

Introduktionsvideo til opgaven: https://youtu.be/F9IvLqyIrTs
Opfølgningsvideo: https://youtu.be/Xq90dDQgles

Feedback tekst til elever
Et brute-force-angreb er en angrebsmetode, som gør brug af metoden *"trial and error"*. Hackere bruger som regel brute-force-angreb til at knække adgangs- eller pinkoder og krypteringsnøgler. Når der foretages et brute-force-angreb prøver banditter hele tiden at sende forskellige data afsted, for at se om data er korrekte. En pinkode er god, fordi den er nem at huske, men pinkoder bliver hurtig skrøbelige, fordi de som regel kun består af fire tal.
En hacker, som vil have adgang til systemer, hvor der bruges en firecifret pinkode skal maksimalt afprøve en kombination af tal 10.000 gange (10^4). Det er derfor vigtigt, at du - når du arbejder med systemer, der gør brug af pinkoder - sikrer dig, at brugeren (hackeren) nægtes adgang efter 3., 4. eller 5. forsøg. Samtidig skal du øge tidsintervallet mellem forsøgene. En anden mulighed er at øge antallet af cifre fra fire til seks i kombination med udelukkelse i en tidsperiode. Det gør det lidt mere besværligt for angriberen, da han nu kan risikere at bruge 1.000.000 (10^6) forsøg. Ifølge ISO 9564 standarden, som er en pin-standard i den finansielle sektor, kan en pinkode ligge mellem fire og 12 cifre, men det anbefales ikke at øge længden til mere end seks cifre, fordi brugere skal kunne huske deres personlige kode.
Hvis det er muligt, øges sikkerheden også for den enkelte bruger, hvis han eller hun ikke selv kan definere sin egen pinkode. Brugere har tendenser til at bruge fødsels- eller andre mærkedage i deres pinkode.

Et levende bevis

… banditterne har sendt et bevis på, at hunden stadig lever i form af et link til en hjemmeside….

Anden opgave i missionen består i at finde oplysninger på en simpel hjemmeside. Denne opgave er designet for, at eleverne kan få kendskab til princippet *"Avoid security by obscurity"* (Merkow & Raghaven, 2010 s.58) og ad den vej lære at holde på en hemmelighed og ikke skjule *"hoveddørsnøglen under dørmåtten".*

I opgaven skal eleverne finde ud af, hvem der har udarbejdet hjemmesiden. Selve opgaveformuleringen kan virke lidt søgt, men den er absolut relevant. Som en del af fagpakken på H1 skal eleverne igennem grundlæggende HTML, CSS og JavaScript, som de kombinerer med et mindre backend-system som regel skrevet i C#. Vi ved, af erfaring, at det er meget svært for eleverne at redegøre for, hvilke dele, som afvikles *server-side* og hvilke dele, der fortolkes af klienten. Vi oplever tit, at de vælger på klientsiden at indsætte følsomme informationer, eksempelvis API nøgler, som potentielt kan være skadelige. Vi håber, at det giver stof til eftertanke og transferlæring[11] hos eleverne, altså at eksponering af tilsyneladende uskyldig information og opbevaring af data i kildekoden på

[11] At eleven kan tage det, lærte og bruge sin viden i en anden kontekst

klientsiden, kan få alvorlige konsekvenser. Eleverne skal forstå, hvad hemmeligheder helt præcist er, hvordan hemmeligheder bliver afsløret, og hvad eleven kan gøre for at beskytte hemmelighederne.

Eleverne skal gerne erfare, at velkendte sandheder som for eksempel, at det er farligt at offentliggøre sine kreditkortoplysninger, også gør sig gældende i kildekoden. Det vil sige, at eleverne bliver bevidste om, at enhver form for data, der er følsom over for en organisation eller person, er hemmelig og ikke bør afsløres offentligt. Det kan være en adgangskode, en adgangsnøgle, et API-token, et kreditkortnummer og meget mere. På sigt ønsker vi, at eleverne fjerner hemmeligheder fra koden og placerer dem i konfigurationsfiler. På senere hovedforløb placeres hemmeligheder i miljøvariabler og value/key container. Eleverne introduceres for lokale scanningsværktøjer[12], som skal afvikles pre-commit til git, og de introduceres til GitHub scanningstjeneste for at fange almindelige hemmeligheder før push accepteres.

Introduktionsvideo til opgaven: https://youtu.be/BmVe8BehWf8
Opfølgningsvideo: https://youtu.be/HgtF4dyoffs

Feedback tekst til elever

Når en applikation udvikles, består programmellet af to dele, en frontend og en backenddel. Og det uanset om der er tale om et websted, en konsol- eller en mobilapplikation,

Frontend-delen er den grafiske repræsentation af din applikation. Det er den del, dine brugere benytter for at interagere med dit system. Backend-delen er selve maskinrummet for dit program. Det er her din forretningslogik er implementeret.

I en webapplikation består frontend'en af HTML, CSS og JavaScript, mens backend typisk er skrevet i f.eks. C#, Java eller PHP.
Når brugeren benytter dit website, gør han det igennem en browser, for eksempel Chrome eller Edge. Browseren forstår ikke særlig meget; den kan kun fortolke HTML, CSS og JavaScript. Når en klient ønsker at se én af dine websider, forespørger han serveren om en specifik side (URL).

Webserverens opgave er at fortolke din backend kode og transformere din C# kode til noget browseren kan forstå. Når du skriver kommentar i enten HTML, CSS eller JavaScript – kan det derfor læses og fortolkes af browseren og dine brugere. Denne del af koden transformeres derfor ikke, da den jo allerede er "læsbar".

Det betyder, at du skal være påpasselig med, hvad du indlejrer i HTML, CSS eller JavaScript, fordi klienten kan altid finde disse informationer. Undgå derfor bl.a. API nøgler, fortrolig information eller brugernavne/password.

[12] truffleHog og/eller git-secrets

Dazebook

… agent X og Y har på baggrund af elevernes information fundet Carlos (Bandit No. 1) Dazebook profil….

Angreb på eller via sociale medier udgør en stor risiko for både enkeltpersoner og virksomheder. Disse angreb kan forekomme på forskellige måder og kan have alvorlige konsekvenser. Eksempler på teknikker, der kan anvendes i angrebene, er *phishing*, spredning af malware og oprettelse af falske profiler. Ofte vil angriberne bruge *Social Engineering* teknikker til at narre brugere til at give følsomme oplysninger eller downloade skadelige programmer. Det er vigtigt at bemærke, at der findes mange forskellige former for *Social Engineering* angreb, og at der hele tiden opstår nye trusler, som man skal være opmærksom på. Det er derfor vigtigt at holde sig opdateret om de seneste trusselsbilleder og beskyttelsesmetoder for at minimere risikoen for at blive offer for et angreb. Flere rapporter og undersøgelser har vist en stigning i forhold til *Social Engineering* angreb på verdensplan. IBM Threat Intelligence rapport (IBM Security, 2022) viser, at *Social Engineering* teknikker er blevet mere udbredte og effektive, og identificerer disse som en af de største trusler mod sikkerheden. Secureworks er en virksomhed, som leverer cybersikkerhedstjenester til store og mellemstore virksomheder, offentlige institutioner og organisationer. De har sponsoreret Boardroom Cybersecurity 2022 rapport (Morgan u.d.), som forudsiger, at de samlede omkostninger ved cyberkriminalitet vil overstige 10 billioner dollars inden udgangen 2025, og at Social Engineering vil udgøre en stadig større del af disse omkostninger. Verizon Data Breach Investigations rapporten (Verizon) er en årlig publikation, der undersøger og identificerer tendenser og mønstre i cybersikkerhedshændelser over hele verden. Rapporten viser, at Social Engineering er den mest almindelige angrebsvektor for datakompromittering.

Argumentet for at lære eleverne noget om Social Engineering, er derfor yderst relevant og vi tager udgangspunkt i Carlos' *Dazebook* profil samtidig med, at eleverne, gennem Agent X og Y, får viden om, hvordan mennesker som udgangspunkt konstruerer deres password. Eleverne bør lære, via praktisk erfaring, at der er mange kendte password mønstre, som er usikre og lette at gætte for en angriber. Nogle af de mest almindelige mønstre inkluderer brugen af simple og almindelige ord som "password" eller "qwerty" ofte med substitutionsmønstre, hvor bogstaver erstattes med tal eller symboler, eller personlige oplysninger som navne på kæledyr osv. Vi vil derfor gerne lære eleverne noget om, hvordan en angriber, gennem Social Engineering teknikker på sociale medier, kan skaffe viden om offerets opførsel, interesser og relationer. Yderligere er det interessant for eleverne at forstå, hvordan denne viden i kombination med gængs passwordadfærd kan bruges til at "gætte" offerets password.

Det er vigtigt, at eleverne forstår vigtigheden af at være forsigtige med at dele personlige oplysninger eller adgangskoder online og samtidig vælge stærke og unikke adgangskoder og regelmæssigt ændre dem for at minimere risikoen for at blive angrebet. Det er også afgørende at være opmærksom på disse metoder og altid være på vagt for at beskytte ens online sikkerhed.

Introduktionsvideo til opgaven: https://youtu.be/CQ4mkvYUukA
Opfølgningsvideo: https://youtu.be/ZPvYT_e5n3Q

Feedback tekst til elever

Social Engineering er atypiske angreb, som du kan blive udsat for, og som hverken virusskannere eller firewalls kan beskytte dig imod. Den slags angreb går i alt sin enkelthed ud på, at angriberen lærer dig at kende, fx via SoMe og ad den vej åbner mulighed for at manipulere dig i en sådan grad, at du ikke aner uråd.

Et eksempel kunne være en angriber, der har undersøgt din profil på Facebook og kan se du holder ferie i Spanien. Han udgiver sig efterfølgende for at være én af dine kollegaer, nabo eller en helt tredje person. Han starter f.eks. samtalen med: "Jeg ved godt, at du holder ferie. Spanien er fantastisk…….. men ". De første sætninger giver dig tryghed for, at vedkommende kender dig.

SoMe bruges altså ikke kun til at vise billeder, tjekke ind på lokationer og følge med i andres liv. SoMe kan også bruges til at skaffe oplysninger om dig, som kan bruges i andre relationer, eksempelvis til at gætte dit password. Husk at hackere er særdeles gode til at finde information og krydsreferere oplysningerne, så de skaber sig et langt større indblik i, hvem du er, og hvordan du nemmest kan manipuleres.

Derfor er det ekstremt vigtigt, at du nøje overvejer, hvilke informationer du ønsker at dele med omverdenen og med hvem. For at undgå at blive udsat for Social Engineering er der flere ting, du selv kan bidrage med. Start med at have en god og fornuftig håndtering af dine passwords. Log ud af dine enheder, når du ikke benytter dem og undersøg for en god ordens skyld altid gerne afsendere af beskeder, som virker legitime, men hvor der er en lille alarmklokke der ringer.

Du kan læse mere om denne form for angreb hos Cyberpilot.

X-files

… man har fundet en FTP server, som muligvis indeholder nogle interessante filer ….

X-files opgaven tager ikke udgangspunkt i noget angreb, men handler langt mere om at, *sikkerheden er aldrig stærkere end det svageste led.* Det eneste, eleverne skal i denne opgave, er at logge ind på en FTP server og hente nogle filer, udfordringen ligger i, at de selv skal gætte brugernavnet og regne ud, at de skal bruge det fremskaffede password fra tidligere. Som refleksion til selve opgaven får eleverne, gennem Fred og Wilma, langt mere information om brugernes adfærd i forhold til passwordkonstruktion. Vi vil gerne have, at eleverne reflekterer over, at mange brugere vælger samme brugernavn og password på tværs af platforme, og hvorfor det kan være en potentiel sikkerhedsrisiko. Samtidig får de gode råd til, hvordan de, i deres softwareimplementeringer, kan hjælpe brugerne med at konstruere mere sikre password ved for eksempel ikke at tillade mønstergentagelser og kontekstspecifikke password, og hvor der løbende kan tjekkes på *"have i been pwned?"*[13]

[13] https://haveibeenpwned.com/

Introduktionsvideo til opgaven: https://youtu.be/HflzXroiiws
Opfølgningsvideo: https://youtu.be/7Zr8Jq8VfVE

Feedback tekst til elever

Når det kommer til sikkerheden, er passwords vores mest fortrukne metode til at sikre autentifikation. Men vi balancerer på en knivsæg.

På den ene side øger brugen af passwords sikkerheden markant i forhold til pinkoder, fordi vi kan gøre passwords længere og mere komplekse. På den anden side kan passwords reducere sikkerheden, fordi der som regel er brugere involveret.

Brugere er med til at reducere sikkerheden på flere fronter, når det kommer til autentifikation. De har tendens til at bruge de samme brugernavne og password på tværs af platforme. Det betyder, at en angriber, der har fået adgang til brugernavnet og passwordet til for eksempel din Twitterkonto, med stor sandsynlighed også kan logge ind på f.eks. Instagram. Endnu værre er det imidlertid, at vi heller ikke skelner mellem vores privat- og arbejdsliv. Har en angriber først adgang til en privat platform, kan han bruge informationerne til også at komme ind på brugerens arbejdsplads og den vej rundt skaffe sig adgang til virksomhedens systemer - og så har vi balladen.
Den måde vi, som mennesker, udformer og designer vores password på, er også en udfordring i forhold til sikkerheden – for vi er slet ikke så smarte, som vi måske selv går og tror.

Vores opgave er at højne sikkerheden i forhold til vores systemer. Vi skal hjælpe brugerne lidt på vej i forhold til deres passwordhygiejne. NIST (National Institute of Standards and Technology) anbefaler, at du gør brug af følgende guide i forhold til passwordhygiejnen hos dine brugere.

- Tjek løbende om brugernes password er lækket. Det kan du selv prøve her: ';--have i been pwned?
- Bloker password, som findes i det man kalder Password Dictionaries. Det kræver dog, at man selv implementere denne funktion og får fat i disse filer
- Forhindr brugere i at benytte sekventielle password, som f.eks. 'aaaaaaaa' eller 'abcdefgh' eller fortløbende nummering. Brugere vælger ofte at skifte et tal i passwordet ud, med næste tal i rækken fra f.eks. P@$$word1 til P@$$word2.
- Undgå at brugere benytter kontekstspecifikke ord i deres password. Det kan være deres brugernavn eller fulde navn eller anden information som systemet kender til deres brugere.
- Øg længden af password til et minimum af otte tegn og gerne flere. Password som er lange, tager længere tid at bryde.

Du kan læse mere om anbefalingerne fra NIST på: Digital Identity Guidelines

Cheese and crackers

… der er fundet 2 interessante filer, som indeholder meget vigtig information for at finde hunden og halsbåndet ….

Eleverne har downloadet de 2 filer fra FTP-serveren, men de er alle adgangskodebeskyttet. Formålet med denne øvelse er at bygge videre på deres viden fra den første opgave omkring brute force angreb. Nu øges tegnsættets størrelse fra at indeholde kun 0-9 til nu også til at omfatte A-Å og a-å. Den ene fil er beskyttet med en passwordlængde på 4 og den anden 6 tegn. Når vi vælger at tage denne opgave med her, er det ikke, fordi vi ønsker, at de skal lære at bryde adgang, men mere fordi vi indimellem har elever, i større organisationer som for eksempel NNIT, der undrer sig over, at både NIST og OWASP kun anbefaler min. 8 tegn, når de nu i deres hverdag er underlagt 12 eller 16.

Vi vil gerne, at eleverne, i denne opgave, reflekterer over, at både længden og tegnsættets størrelse har en betydning i forhold til brute force angreb, og at tiden er en væsentlig faktor. Øvelsen opfordrer eleverne til at gøre brug af eksterne værktøjer til at bryde adgangen for at undgå at sidde fast i forhold til kompleksitet. I den efterfølgende refleksionsvideo præsenteres eleverne for konkrete anvisninger i forhold til længde og tegnsættets størrelse. Disse fakta skal være med til at underbygge elevens læringsstil.

Introduktionsvideo til opgaven: https://youtu.be/VwZl8FyRu6U
Opfølgningsvideo: https://youtu.be/l_FzGmFQu_k

Feedback tekst til elever
At tillade flere tegn i hver "position" i en adgangskode øger kombinationsmulighederne, hvilket betyder, at et brute-force-angreb kan tage længere tid at gennemføre.

Har du et for eksempel en adgangskode på fem tegn og bruger du alle 29 tegn (lower case) i det danske alfabet, findes der 29^5 kombinationsmuligheder (29 x 29 x 29 x 29 x 29). Det svarer til omkring 20 millioner kombinationer.

Øger du tegnsættet til også at indeholde store bogstaver, altså 58^5, så øges antallet af kombinationer til omkring 656 millioner. Tilsætter du f.eks. tal (0-9) og 10 symboler, så får du 78^5 kombinationsmuligheder, hvilket er omkring 2,8 milliarder.

Så størrelsen på tegnsættet har betydning, men måske er det langt vigtigere også at se på længden.
At have store nøglelængder (flere anslag) gør, at et brute-force-angreb kan tage væsentlig længere tid.
Med 29 tegn og passwordlængde på tre tegn (29^3), er der 24.000 mulige kombinationer. Øger du længden til otte tegn (29^8), så har du omkring 500 milliarder kombinationer.

En skjult besked

… zip-filerne er cracket, indeni ligger nogle snapshots af hunden på tur i parken og ikke andet….eller?

Eleverne er meget interesseret i kryptografi, det ser vi i hvert fald tit i undervisningen, men også under vores interviews. Det er derfor en rigtig god anledning til at introducere dette emne. Igen er det vigtigt at holde elevernes kompetenceniveau indenfor øje. Det kan være svært at arbejde med krypteringsalgoritmer og hashing, når eleverne dårligt ved, hvordan en for-løkke fungerer. Vi har derfor nøje overvejet, hvordan vi skulle gribe kryptering og hemmeligheder an, og valget er blandt andet faldet på steganografi. Som overordnet formål vil vi gerne gøre eleverne opmærksomme på, at ikke alt er, hvad det udgiver sig for at være. Steganografi anvendes til kriminalitet på forskellige måder. I september 2020 opdagede det hollandske sikkerhedsfirma Sansec (Hunter, 2022), at cyberkriminelle grupper benyttede sig af billede-steganografi til at stjæle kortoplysninger fra online butikkers betalingsside via malware indlejret i SVG filer. Angrebet, der kaldes *skimming*, er en almindelig metode, hvor angriber indsætter ondsindet kode i en forhandlers betalingsside. Sansec's

grundlægger, Willem de Groot, har udtalt (Sansec, 2019), at firmaet har opdaget, at mere end 50.000 online butikker er blevet ofre for denne type af malware.

Refleksionsteksten på platformen inkluderer en kort video, hvor elever kan se, hvor let det er at oprette en tilsyneladende uskyldig billedfil, der, når filen bliver maksimeret, eksekverer en (uskyldig) virus/malware. Formålet med denne video er at vække elevernes nysgerrighed og give dem motivationen samt vi får en fælles reference til senere hovedforløb, hvor de vil arbejde med udvikling af webapplikationer, der inkluderer en upload-komponent. Gennem sikkerhedsforanstaltninger vil eleverne opnå en forståelse for vigtigheden af at følge grundlæggende regler ved implementering af filupload (Ullrich, 2009) for at sikre en stærk sikkerhedskonfiguration. Elevernes forståelsesramme bør inkludere, at steganografi i sig selv ikke er en forbrydelse, men teknologien kan anvendes ondsindet. Derfor er det afgørende at have passende sikkerhedsforanstaltninger på plads for at opdage og forhindre denne type misbrug af steganografi.

Introduktionsvideo til opgaven: https://youtu.be/ReCB-hUP2MI
Opfølgningsvideo: https://youtu.be/bdizULL2_Nk

Feedback tekst til elever

Steganografi et alternativ til kryptografi
Steganografi er kunsten *at skjule* eksistensen af en besked eller et budskab. Steganografi er relateret til, men forskelligt fra, kryptografi. Formålet med steganografi at beskytte/skjule indholdet af en meddelelse. I modsætning til kryptografi er indholdet af beskeden dog ikke krypteret. I stedet er meddelelsens eksistens skjult i et andet kommunikationsmedie. Kommunikationsmediet kan for eksempel være en protokol, et digitalt billede, et lageringsmedie eller en lydfil. Steganografi kan forstås som teknikken til at skjule/indkapsle data i en almindelig, ikke-hemmelig besked eller fil, som man kalder coverfilen.

Hvordan virker Steganografi
Indlejringsprocessen kan udføres ved hjælp af forskellige teknikker, hvor en af de mest almindelige er Least Significant Bit (LSB) steganografi. Processen involverer indlejring af den hemmelige besked i de mindst signifikante bits i coverfilen, for eksempel et billede af typen .JPEG. En digital billedfil består af farverne blå, rød og grøn, og hver pixel indeholder tre bytes. LSB-teknikken hjælper med at transformere den sidste bit af hver af disse bytes for at skjule en bit data. Ændringen af den sidste bits pixelværdi medfører ikke nogen mærkbar ændring i billedet – set med det menneskelige øje.

Angreb og steganografi
Angribere udnytter steganografi til en række forskellige angreb, eksempelvis til at skjule ondsindede payload og scriptfiler. Malware-udviklere benytter ofte LSB-steganografi til at skjule den ondsindede kode i billeder af nøgne damer og eller populære sange. Den skjulte malware eksekveres herefter af en anden applikation eller service, efter at coverfilen er downloadet på offerets computer. Udtrykket *en trojansk hest* anvendes ofte til at beskrive en ondsindet fil, som er lageret i en harmløs fil. Steganografi anvendes i dag kreativt af angribere, når der er behov for at omgå beskyttelsesmekanismer, såsom begrænset filupload. De kriminelle hackere er dog ikke de eneste aktører, der anvender steganografi. Spioner og aktivister anvender teknikken til at kommunikere med deres organisationer for at undgå at vække mistanke hos myndighederne.

Detektion af steganografi
Kunsten at detektere steganografi kaldes steganalyse, tilsvarende er kryptoanalyse anvendt på kryptografi. Der er flere værktøjer, der kan registrere tilstedeværelsen af skjulte data, såsom StegExpose og StegAlyze. Nogle analytikere bruger andre analyseværktøjer, såsom hex-viewere til at opdage uregelmæssigheder i filer.

Verden i dag
Cyberspionagegrupper har fornyelig benyttet et steganografi til at skjule en bagdør/spyware i Windows-logoet. Du kan læse mere her Windows logo

DYI
Du kan selv prøve at lave dit eget lille hack Kik her

Substitutten

… banditterne er i gang med en live-chat …. men pludselig, når det bliver allermest spændende, krypteres beskederne…

Hovedkontoret har fået opsnappet en live-chat, som eleverne får adgang til gennem et link. Beskederne er i starten rimelig uskyldige, men på et tidspunkt krypteres informationerne. Det er nu elevernes opgave at bryde disse kodede beskeder og hive essensen ud af dem, så de kan skaffe nøglen og bevæge sig videre på platformen. Der gives kun én oplysning om selve krypteringsnøglen, og det er +12. Her er der selvfølgelig tale om en simpel Cæsar kryptering. Når vi vælger denne kryptering, er det fordi, at den er enkel, simpel, nem at forstå, let at bryde, og den giver et godt indblik i de grundlæggende principper i forhold til den symmetriske kryptografi. Vi vil gerne, at eleverne efterfølgende får tænkt over de potentielle katastrofale konsekvenser, der kan opstå, når nøglen er offentlig kendt. Vi tænker, at denne refleksion opstår når eleverne forsøger at bryde de krypterede chat-beskeder, og de ser hvor let, det egentlig er. I den efterfølgende refleksionsvideo forsøger Wilma at give et indblik i et par krypteringsmetoder samt forklare forskellen på den symmetriske og asymmetriske kryptering og trække paralleller til den virkelige verden i forhold til https-protokollen, som eleverne kender til.

Introduktionsvideo til opgaven: https://youtu.be/-6XiutvWdGM
Opfølgningsvideo: https://youtu.be/uQnzWJHVEw4

Feedback tekst til elever

Du har nu lige prøvet at bryde en kryptering. Den var faktisk ikke så svær. Cæsarkoden opstod tilbage i tiden, under kejser Julius Cæsar. Han brugte denne form for kryptering til at sende hemmelige beskeder afsted til sine generaler.

Selve kodeformen kaldes en monoalfabetisk kode, hvor man roterer alfabetet enten frem eller tilbage. Koden er ikke særlig sikker og kan nemt "brute forces". Antallet af kombinationsmuligheder afhænger af antallet af tegn, der bruges i tegnsættet.

Har du brug for at kryptere data, er det derfor vigtigt, at du benytter dig af standardiserede

krypteringsalgoritmer fremfor at bruge svage algoritmer eller udvikle dine egne.
For at krypteringen kan opretholde en "høj" sikkerhed, skal algoritmen være robust. Robusthed sker ikke automatisk. Det tager tid før en krypteringsalgoritme kan blive anerkendt.

At have en krypteringsalgoritme er kun en del af en større helhed, når det kommer til at sikre data. Der er mange gode grunde til, at hjemmeudviklede krypteringsalgoritmer ikke er noget, der er let at gå i gang med og som skal undgås. Kryptering er en meget vigtig sikkerhedsforanstaltning. Uden et meget grundigt kendskab til systemdesignet og de underliggende matematiske principper, som ofte kræver mange års uddannelse og erfaring. Heldigvis har vi allerede en række krypteringsalgoritmer, der testes i produktion af et globalt publikum. På grund af eksistensen af afprøvede og pålidelige krypteringssystemer, ser vi langt færre hjemmeudviklede krypteringsalgoritmer, i modsætning til tilbage i 80'erne, hvor det var en almindelig praksis.

Under konstruktion

… De slemme fyre har købt jackal.com, og vi har brug for MAC-adressen… deres hjemmeside har heldigvis en fejl….

På det første hovedforløb har eleverne begrænset erfaring med fejlhåndtering, og deres primære fokus er at producere fungerende kode med det ønskede output. Eleverne får en introduktion til fejlhåndtering både i forhold til segmentering og logning af fejl. Vi oplever ofte, at eleverne kun anvender en blok, der fanger alle fejl, hvilket ofte resulterer i mangelfuld behandling og logning af fejl(ene). Gang på gang ser vi elevers fejbeskeder indeholde detaljerede oplysninger om programmet, dets konfiguration eller brugeridentificerende oplysninger.

Selvom introduktionen til fejlhåndtering er nyttig, giver den ikke altid eleverne en dybere forståelse af, hvordan de kan identificere og løse fejl via fejlhåndtering – måske fordi undtagelseshåndtering er en kontinuerlig proces, der kræver erfaring og øvelse og derfor foregår over mange hovedforløb.

Vi ønsker gennem princippet Fail Securely (Merkow & Raghaven, 2010 s. 58), at eleverne vil blive bedre til at identificere og løse fejl og tage ansvar for deres kode. I øvelsen bliver eleverne opmærksomme på betydningen af forkert fejlhåndtering fra undtagelsessystemet, som har tendens til at give mere information, end det er nødvendigt. Standardfejlbeskederne skal erstattes med en mere sikker tilgang og bør føre til en forståelse af, at de detaljerede fejlmeddelelser skal skrives til en log, hvorimod slutbrugeren modtager meningsfulde og forståelige fejlmeddelelser, som ikke afslører informationer omkring systemet. En anden vigtig pointe, som eleverne skal tage med fra øvelsen, er, at undtagelseshåndtering ikke i sig selv forårsager skade, men snarere tillader angribere at afdække angrebsoverfladen via fejlbeskederne. Omdrejningspunktet for fejlbeskeder i opgaven er kommando-injektion gemmen et websted, hvorpå serverens MAC-adresse findes og udskrives til en tekstfil, der herefter kan tilgås gennem *directory browsing* på web-serveren.

Introduktionsvideo til opgaven: https://youtu.be/0MAS8r3NJ_0
Opfølgningsvideo: https://youtu.be/yJTSDEQclmU

Feedback tekst til elever

Forståelse af fejlmeddelelser er en vigtig del i alle programmeringsopgaver. Webapplikationer er specielt sårbare, når det kommer til forkert fejlhåndtering pga. det globale publikum. Fejlmeddelelser giver værdifuld information til programmøren, når der sker en undtagelse (fejl). Informationen giver udvikleren mulighed for at løse og hermed forbedre brugeroplevelsen. Desværre kan det ske, at når fejl ikke håndteres korrekt, og at følsomme oplysninger blive afsløret. Det fører igen til sårbarheder, der udnyttes af angribere. Ukorrekt fejlhåndtering opstår, når den fejlmeddelelse, der vises til slutbrugeren, giver et fingerpeg om, hvordan en applikation eller en hjemmeside fungerer. Selvom fejlbeskeder kan hjælpe programmørerne med at løse problemer, vises fejlbeskederne også til angribere. Hackere benytter disse oplysninger, når de bryder ind i ellers sikrede systemområder. For eksempel kan en fejlmeddelelse, der indeholder oplysninger om strukturen af en databasetabel, give angribere alt, hvad han/hun behøver af viden for at udføre et vellykket SQL-injektionsangreb. Et andet eksempel er en fejlbesked, hvor man kan se, at en proces er påbegyndt baseret på brugerinput. Dette kan medføre, at en angriber kan udføre kommandoer, der fortolkes af operativsystemet.

Hvornår opstår forkert fejlhåndtering?

Når fejlmeddelelser indeholder detaljer, der kan være nyttige for en angriber, er det forkert fejlhåndtering. I mange tilfælde er forkert fejlhåndtering et resultat af, at der benyttes standardiserede fejlbeskeder fra undtagelseshåndteringen (try/catch). Disse meddelelser kan indeholde detaljerede oplysninger om filsystemet eller be- eller afkræfte, at der findes filer og mapper. Nogle af standardbeskeder i .NET indeholder oplysninger om serversoftwareversionen, mens andre beskriver, hvor konfigurationsfiler er placeret eller stack trace detaljer.

En angriber kan bruge disse oplysninger til at udlede viden omkring dit system. Et typisk eksempel kunne være, at brugeren får en *access-denied* på et bestemt objekt, for eksempel en fil. Ved at give denne fejlbesked, har systemet samtidigt bekræftet af objektet eksisterer.

Fejlhåndtering er ikke farligt

Håndtering af fejl forårsager ikke skade i sig selv. De tillader snarere angribere at afdække sårbarheder eller angrebsvinkler, som angribere kan bruge til at udnytte andre system- og/eller kodefejl. Dette gør fejlhåndteringsangreb til en form for rekognoscering, hvor angribere analyserer webapplikationer eller andre systemer for svage punkter, før de bryder ind og stjæler data eller forårsager skade.

Hvad skal du gøre fra i dag

Mange håndteringsfejl kommer som beskrevet fra standard fejlbeskeder fra undtagelsessystemet. Fejlbeskederne har tendens til at give mere information, end det er nødvendigt for slutbrugerne. Erstat derfor standardbeskeder med en mere sikker tilgang. Hvis der kræves detaljerede fejlmeddelelser til programmøren, skrives disse til en logfil i stedet, mens slutbrugere får en mere venlig besked, der undgår at afsløre følsomme oplysninger. Et andet vigtigt aspekt ved fejlhåndtering er konsistens. Programmører bør udføre en detaljeret kodegennemgang af fejlhåndteringslogikken i deres kode og sikre korrekt fejlhåndtering. OWASP definerer korrekt fejlhåndtering som den, der giver *"en meningsfuld fejlmeddelelse til brugeren, diagnostisk information til webstedets vedligeholder og ingen nyttig information til en angriber"*.
Læs mere hos OWASP

Medianen

… Hundens halsbånd udsender lokationsdata til en server! Find serveren og bagdøren til systemet…

Grundlaget for denne opgave er, at eleverne - via et værktøj, eksempelvis Nmap, scanner netværket og finder ud af, hvilke netværksservices, der afvikles på hvilke porte. Herefter udvikles en lille applikation, der forbinder til porten og modtager data. Læringen i opgaven er at forstå, at fejlkonfigurerede porte åbner en bagdør til miljøet. Sikkerheden for netværksapplikationer afhænger b.la af forståelsen om, hvordan porte benyttes, konfigureres jf. OWASP top10 og ikke mindst, hvordan de sikres. Sikkerhedsforståelsen for porte er ekstremt vigtig, specielt når de er internetvendte. Åbne porte er en potentiel angrebsåbning. Processen skulle gerne give viden om, at åbne porte ikke er problemet i sig selv. Det er applikationerne og tjenesterne, der lytter på disse porte, som udgør problemet.

Porte udgør en integreret del af netværksinfrastrukturen og har til formål at dirigere trafikken mellem forskellige enheder og applikationer på netværket. Denne del udgør et essentiel erfaringsgrundlag for eleverne, hvilket kan lette deres beherskelse af emnet på senere stadier af deres uddannelsesforløb. Såfremt eleverne skal fungere som sikkerhedsambassadører, er det vigtigt, at de tilegner sig de grundlæggende sikkerhedsprincipper allerede på første stadie af deres uddannelsesforløb. Et af disse principper er *least privilege,* og vi håber, at ved at forstå og anvende princippet, kan eleverne bidrage til beskyttelsen af deres programmer og systemer mod sikkerhedstrusler og -brud. Ofte overtrædes sikkerhedsprincippet *least privilege*, når eleverne udvikler deres programmer i forbindelse med blandt andet brugerrettigheder, adgangskontrol, kodeeksekvering samt netværks- og dataadgang. Elever kan bryde sikkerhedsprincippet *least privilege* i deres programmering af forskellige årsager, herunder primært en mangel på erfaring og viden om sikkerhed samt gode praksisser inden for programmering. Elever på første stadie af deres uddannelsesforløb fokuserer typisk mere på at opnå funktionalitet fremfor at overveje sikkerhedskonsekvenserne af deres kode.

Introduktionsvideo til opgaven: https://youtu.be/-BWQ17NzRjg
Opfølgningsvideo: https://youtu.be/3m3PuH5oNCs

Feedback tekst til elever

En åben port er en softwaredefineret værdi, som identificerer et end-point i en infrastruktur. Enhver forbindelse på et TCP/IP-baseret netværk har en kilde- og destinationsport. Porten anvendes med de respektive IP-adresser til entydigt at identificere afsender og modtager af hver datapakke. Porte er afgørende for TCP/IP-baseret kommunikation. Fejlkonfigurerede porte og port-sårbarheder åbner en bagdør til miljøet, hvor applikationen afvikles. Sikkerheden for applikationer afhænger blandt andet af forståelsen om, hvordan porte benyttes, og hvordan de sikres. Sikkerhedsforståelsen for brug af porte er ekstremt vigtig, når de er internetvendte.

På trods af, at porte er alt afgørende for, at et TCP/IP-baseret netværk fungerer, er åbne porte en potentiel angrebsåbning. Åbne porte er ikke problemet i sig selv. Det er applikationerne og tjenesterne, der benytter disse porte til kommunikation, som udgør problemet. Angribere kan nemt udnytte svagheder i disse applikationer. Angribere kan drage fordel af sikkerhedssårbarheder i ældre, ikke-patchet software, svage

legitimationsoplysninger og forkert konfigurerede tjenester til at kompromittere et netværk eller en applikation.

Nogle porte er ikke beregnede til at blive offentligt eksponeret. For eksempel er SMB-protokollen, som fungerer over TCP-porte 139 og 445, åben som standard på Windows-platforme. Porten er kun beregnet til fildeling, printerdeling og fjernadministration. Der har været adskillige sårbarheder i de tidligere versioner af SMB-protokollen, som er udnyttet af angribere med blandt andet *WannaCry-ransomware*. Computere inficeret med WannaCry-koden scannede deres netværk for enheder, der accepterede trafik på SMB-porte for at oprette forbindelse til dem og sprede ondsindet software.

Derudover er nogle porte mere tilbøjelige til at blive angrebet. Et eksempel er Microsofts fjernskrivebordsprotokol (RDP), som giver en bruger mulighed for at få adgang til en fjernvært.

Hvad kan du gøre for at minimere porte, som er relateret til risici i et softwaremiljø? Det vigtigste er at identificere og overvåge alle åbne porte. Løbende skal der kontrolleres for eventuelle port-relaterede konfigurationsændringer. Lige så vigtigt er det at forstå og dokumentere al brug af porte på tværs af dit miljø. Disse oplysninger giver en baseline for port-sikkerhed. På baggrund af konkret trusselsvurderinger kan andre elementer implementeres. Det kunne være multi-faktorautentificering, netværkssegmentering, anvendelse af princippet om "Least privilege" med mere.

Konklusion

Når vi ser på, hvordan vi tidligere har arbejdet med softwaresikkerhed som begreb, og gjort brug af modeller i undervisningen, så er der et gab mellem elevernes læring og vores forventede udbytte, især når det kommer til begrebsforståelsen. Samtidig har vi, om end datagrundlaget for vores eksperiment er relativt småt, kunne se en tendens til, at eleverne havde mere fokus på sikre implementeringer, når de havde fået en praktisk erfaring med at angribe et eksisterende system, fremfor de elever, der kun havde fået en "teoretisk" gennemgang. Det går godt i tråd med ZBC's didaktiske grundlag, som understreger, at eleverne skal arbejde med stoffet ud fra en problembaseret og praksisorienteret kontekst fremfor den klassiske forelæsningsmetodik.

Elevernes faglige niveau og forudsætninger sætter en række begrænsninger i forhold til, hvordan vi skal gribe undervisningen an, både i forhold til differentiering og for at få det optimale udbytte af sikkerhedsundervisningen. Den gennemsnitlige datatekniker elev hører til generation Z, som fortrækker at lære og arbejde i deres eget tempo og primært gennem visuelle materialer og som blandt andet drives af nysgerrighed og motiveres gennem belønninger og feedback. For at engagere eleverne i softwaresikkerhed er det vigtigt at skabe relevans for emnet og vise dets betydning for deres fremtidige karriere og dagligdag. Dette kan gøres ved at forklare, hvordan softwaresikkerhed er en vigtig del af moderne teknologi, og hvordan det kan påvirke dem og deres virksomheder, hvis ikke det implementeres i deres systemer.

Udarbejdelsen af vores platform "*Mission possible*" tager afsæt i konceptet Gamification, som er en effektiv metode til at lære nyt og ændre på eksisterende adfærd gennem brug af konkurrenceelementer, belønningssystemer og øjeblikkelig feedback. Gennem udarbejdelse af vores platform, har vi skabt et motiverende og engagerende læringsmiljø, som kan transformere et til tider tørt og teoretisk emne, som softwaresikkerhed, til noget mere spændende og underholdende. Platformen og indholdet er designet ud fra elevernes faglige, sociale og psykiske forudsætninger, som giver rig mulighed for den praktiske tilgang til læring, der er afgørende for denne elevgruppes læringsudbytte.

Platformen tager udgangspunkt i konkrete missioner, som eleverne selvstændigt skal løse undervejs. Indholdet består primært af visuelle materialer som video, animationer og infografikker, som skal hjælpe eleverne med at forstå komplekse koncepter, begreber og sikkerhedstrusler.

Missionerne er skabt på baggrund af en historiefortælling og opgaverne, som ligger placeret i missionerne har en naturlig progression. Historiefortællingen skal være med til at skabe en illusion til eleverne om, at de er "*superhelte*", som skal være med til at redde verden. Dette element kan være med til, at eleverne føler sig engageret og involveret i deres egen læring. Der er plads til alle elever på platformen også de fagligt svage og uerfarne. De kan arbejde i deres helt eget tempo uden konkurrenceelementet, og går de i stå, er der hjælp at få undervejs gennem ledetråde. I takt med, at eleverne løser en opgave, tildeles eleverne med stjerner og mulighed for at låse op for næste opgave i missionen. Denne tilgang giver eleverne en følelse af progression og belønning, hvilket øger deres motivation til at lære mere om emnet.

Alt i alt, er det tydeligt, at der er et stort potentiale i at anvende gamification og en praksisorienteret tilgang til softwaresikkerheden i forhold til elevernes læring, så de er rustet til at håndtere de udfordringer, de vil møde i deres fremtidige karriere.

Perspektivering

At udarbejde en digital læringsplatform har ikke været en triviel proces, og det har været langt mere omfattende end først antaget. Udover det omfattende videomateriale, design af mission, materialer og tilhørende opgaver, har vi også skulle praktisere det, vi forsøger at lære vores elever i forhold til softwaresikkerheden. Selvom de funktionelle krav til platformen har vist sig at være relativt begrænset, har sikkerhedskravene været ret så omfattende. Man kunne jo sagtens forestille sig, at vi havde elever, som ville forsøge at hacke selve platformen.

Målet for platformen er, at den skal bruges aktivt i undervisningen som et laboratorie, hvor eleverne, i ro og mag, kan arbejde med softwaresikkerheden i praksis. Selvom vi, i første udgave, kun har en mission henvendt til første hovedforløb, så ligger der på tegnebrættet allerede to færdig designet missioner – en til SQL injection baseret på vores tidligere opgave Weapons4U, og missionen Brussel t/r, som omhandler websikkerhed i praksis i forhold til forskellige typer af injektionsangreb. Vi har designet platformen til at være fleksibel, hvilket betyder, at det er nemt at tilføje og fjerne missioner ad hoc. Denne fleksibilitet giver os mulighed for at tage fat i højaktuelle sikkerhedsemner eller designe en mission ud fra klassens eller holdets aktuelle faglige niveau, hvis vi ser, at der er et konkret behov for ekstra tiltag eller områder, der kræver særlig opmærksomhed.

Vi har dog enkelte bekymringer, som vi bør lade eleverne komme til gode, og det er brugen af gamification som metodik. Vi kan godt være lidt bekymret over, om denne platform kommer til at have den modsatte effekt end det, vi forsøger at opnå. Nogle af vores elever stræber efter at vise os, og resten af klassen, hvor dygtige de er – det ser vi ofte i hverdagen. Denne type elever kan muligvis, gennem deres adfærd, demotivere andre elever ved at fortælle dem, hvordan de skal løse opgaverne eller ved at give dem nøglen til næste mission. Derfor ville det være interessant at se på en opgradering af vores platform, så den understøtter differentierede og adaptive opgaver i en mission, så den knapt så dygtige elev kan træne den samme færdighed i forskellige kontekster, og sværhedsgraden øges for den dygtige elev. For at skabe en støttende læringskultur er det vigtigt, at vi sammen får skabt et positivt læringsmiljø, hvor eleverne føler sig trygge ved at stille spørgsmål, eksperimentere og begå fejl.

En anden udfordring er, at eleverne faktisk ikke lærer så meget, og der er en potentiel risiko for, at eleverne fokuserer for meget på belønninger i stedet for reel læring, hvilket resulterer i en overfladisk forståelse af emnet og mangel på motivation til at lære mere efter indfrielse af en belønning. Det er derfor ekstremt vigtigt, at eleverne har fokus på selve læringsprocessen og er motiveret for at dykke dybere ned i emnet ved at stille spørgsmål, udforske forskellige perspektiver og skabe forbindelser til tidligere læring omkring softwaresikkerhed. Derigennem fremmes kritisk tænkning, problemløsning og refleksion, hvilket bidrager til en dybere forståelse omkring et sikkerhedsemne.

En sidste udfordring er, om de opgaver, vi stiller eleverne, er for langt væk fra virkeligheden og deres konkrete hverdag, og at det derfor enten ikke er meningsgivende for dem at løse opgaverne eller at de ikke kan tage deres nye viden og bruge den i en virksomhedskontekst. Det er derfor vigtigt for os at opfordre eleverne til løbende at reflektere over deres egen forståelse og udfordre dem i forhold til deres lærepladser og de systemer, de arbejder med i hverdagen.

Bibliografi

Bakar, P. A. (2022, 3 31). *how can gamification go wrong?* Retrieved from https://www.linkedin.com/: https://www.linkedin.com/pulse/how-can-gamification-go-wrong-puteri-aisyah-radin-abu-bakar/

Bista, G. (2020). Et opgør med nyttetænkningen. In U. m. læring, N. Katznelson, N. Sørensen, & K. Illeris (Eds.). København: Hans Reitzels forlag.

Bulao, J. (2023, 2 27). *How Many Cyber Attacks Happen Per Day in 2023?* Retrieved from Techjury: https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref

Burke, B. (2016). *Gamify.* Ney York: Routledge. doi:https://doi-org.zorac.aub.aau.dk/10.4324/9781315230344

Børns vilkår. (2022). *Ungetrivselsanalyse.* Børns vilkår. Retrieved from https://www.dsfnet.dk/wp-content/uploads/2022/06/Ungetrivselanalyse-Ungetrivselsraadet-maj-2022.pdf

Center for Cybersikkerhed. (2023, 2 20). *Cybertruslen mod Danmark*. Retrieved from Center for Cybersikkerhed: https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Cohen, E. (2011, 6 23). *Does life online give you 'popcorn brain'?* Retrieved from cnn.com: http://edition.cnn.com/2011/HEALTH/06/23/tech.popcorn.brain.ep/index.html

Consumer Insights, Microsoft Canada. (2015). *Attention spans.* Retrieved from https://dl.motamem.org/microsoft-attention-spans-research-report.pdf

DTU. (2019, 4 15). Abundance of information narrows our collective attention span. *EurekAlert!* Retrieved 2 24, 2023, from https://www.eurekalert.org/news-releases/490177

Gartner. (n.d.). *Gamification*. Retrieved from https://www.gartner.com/: https://www.gartner.com/en/marketing/glossary/gamification

Hiim, H., & Hippe, E. (1999). Elevernes læringsforudsærtninger. In H. Hiim, & E. Hippe, *Undervisningsplanlægning for faglærere* (2 ed.). København: Gyldendal.

Homeschool blog. (2022, 07 12). Logical Learner: Characteristics, Strategies, & Activities. Retrieved from https://blog.bjupress.com/blog/2022/07/12/logical-learner-characteristics-strategies-and-activities/

Hunter, T. (2022, 9 22). *Steganography: The Undetectable Cybersecurity Threat*. Retrieved from Built in: https://builtin.com/cybersecurity/steganography

IBM Security. (2022). *X-Force Threat Intelligence Index 2022.* Retrieved from IBM.com: https://www.ibm.com/downloads/cas/ADLMYLAZ

Illeris, K. (2015). *Læring* (3 ed.). Frederiksberg C: Samfundslitteratur.

Institut for Elektroniske Systemer. (n.d.). *Haaukins - Training Platform for Cyber Security*. Retrieved from Aalborg universitet: https://vbn.aau.dk/da/equipments/haaukins-training-platform-for-cyber-security

Jackson, C. (2020). Frygten for fiasko. In N. Katznelson, N. Sørensen , & K. Illeris (Eds.), *Unges motivation og læring.* København: Hans Reitzel.

Katznelson, N., Sørensen, N., & Illeris, K. (2021). *Unges motivation og læring* (2 ed.). Københavh: Hans Reizals forlag.

Kristensen, C. J., & Hussain , A. M. (2016). *Metoder i samfundsvidenskaberne.* København.

Marzullo, D. (2020, 06). *How To Motivate Generation Z At Work.* Retrieved from ProQuest.

Merkow, M. S., & Raghaven, L. (2010). *Secure and Resilient Software Development.* Boca Ranton: CRC Press.

Microsoft. (2021, 8 26). *Widespread credential phishing campaign abuses open redirector links*. Retrieved from Microsoft.com: https://www.microsoft.com/en-us/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

Morgan, S. C. (n.d.). *BOARDROOM CYBERSECURITY 2022 REPORT.* Retrieved from Secureworks: https://content.secureworks.com/-/media/Files/US/Reports/Secureworks_NC2_BoardroomCybersecurityReport.ashx?modified=20220809161846

Nieżurawska, J., Kycia, R. A., & Niemczynowicz , A. (2023). *Managing Generation Z.* Routledge. doi:10.4324/9781003353935

Purcell, K., Rainie, L., Buchanan, J., Friedrich, L., Jacklin, A., Chen, C., & Zickuhr, K. (2012, 11 1). How Teens Do Research in the Digital World. *Pew Research Center*. Retrieved from https://www.pewresearch.org/internet/2012/11/01/how-teens-do-research-in-the-digital-world/

Retsinformation. (2023, 03 22). *Bekendtgørelse om data- og kommunikationsuddannelsen*. Retrieved from Retsinformation: https://www.retsinformation.dk/eli/lta/2023/312

Rothman, D. (2016). A Tsunami of Learners Called Generation Z. Retrieved from https://mdle.net/Journal/A_Tsunami_of_Learners_Called_Generation_Z.pdf

Rymann, E. (n.d.). *Børn og unges læsning 2021*. Retrieved from Center for Anvendt Skoleforskning: https://www.ucl.dk/cas/projekter/boerns-laesning

Sansec. (2019). *Sansec at Europol training: 50,000+ stores hacked*. Retrieved from Sansec: https://sansec.io/news/sansec-europol-training-payment-fraud

Seemiller , C., & Grace, M. (2016). *Generation Z Goes to College* (1 ed.). ProQuest Ebook Central: John Wiley & Sons, Incorporated.

Seemiller, C., & Grace, M. (2018). *Generation Z: A Century in the Making.* London: Routledge. doi:https://doi-org.zorac.aub.aau.dk/10.4324/9780429442476

Skaalvik, E. M. (2020). De usynliggjorte fremskridt. In N. Katznelson, N. Sørensen, & K. Illeris (Eds.), *Unges motivation og læring* (2 ed.). København: Hans Reitzels forlag.

Slade-Silovic, O. (2018, 6 26). *5 Reasons Why Video Content Works Better Than Text*. Retrieved from Covideo: https://www.covideo.com/why-video-content-works-better-than-text/

Statista. (2022, 12 2). *Estimated cost of cybercrime worldwide from 2016 to 2027*. Retrieved from Statista.com: Estimated cost of cybercrime worldwide from 2016 to 2027

Statista.com. (n.d.). Retrieved from Distribution of web application critical vulnerabilities worldwide as of 2022: https://www.statista.com/statistics/806081/worldwide-application-vulnerability-taxonomy/

Time 4 learning. (n.d.). Retrieved from Logical Learning Style: https://www.time4learning.com/learning-styles/logical-mathematical.html

Uddannelses- og forskningsministeriet. (2020, 12 17). *Kvalifikationsrammer \ Niveau 5*. Retrieved from Niveauer i kvalifikationsrammen: https://ufm.dk/uddannelse/anerkendelse-og-dokumentation/dokumentation/kvalifikationsrammer/niveauer-i-kvalifikationsrammen/niveau-5

UddannelsesGuiden. (n.d.). *Skoleoplæring*. Retrieved from UddannelsesGuiden: https://www.ug.dk/uddannelser/artikleromuddannelser/omerhvervsuddannelser/skoleoplaering

Ullrich, D. J. (2009, 12). *8 Basic Rules to Implement Secure File Uploads*. Retrieved from Sans: https://www.sans.org/blog/8-basic-rules-to-implement-secure-file-uploads/

Verizon. (n.d.). *Data breach investigations report.* Retrieved from Verizon: https://www.verizon.com/business/resources/T170/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Wong, C. (2022, 10 1). *How To Make A Flipped Classroom Video*. Retrieved from Panopto: https://www.panopto.com/blog/how-to-make-flipped-classroom-video/

ZBC. (2018). *Fælles pædagogisk.* Retrieved from ZBC.dk: https://www.zbc.dk/media/1810/faelles-paed-didak-grundlag-2018.pdf

Aarhus universitet. (n.d.). *Eksperimenter*. Retrieved from Metodeguiden: https://metodeguiden.au.dk/eksperimenter

Alle billeder som vi ikke selv har fremstillet og brugt i rapporten, på platformen og videomateriale, er hentet fra Freepik.com under en Premium licens, hvilket betyder, at vi må manipulere indholdet efter forgodtbefindende.

https://www.freepik.com/free-vector/cute-cats-playing-with-ball-yarn-cartoon-illustration-set-adorable-baby-kitten-having-fun-enjoying-lying-sitting-standing-hind-legs-domestic-animal-pet-concept_26921604.htm

https://www.freepik.com/free-vector/facebook-web-interface-with-minimalist-design_2401868.htm

https://www.freepik.com/premium-vector/old-mobile-phone-vector-design_31826478.htm

https://www.freepik.com/premium-vector/different-people-crowd-isolated-man-woman-with-gadgets-book-happy-confused-displeased-vector-characters_15865450.htm

https://www.freepik.com/free-vector/corporate-gender-distribution-statistics-vector_3530028.htm

https://www.freepik.com/free-vector/flat-hand-holding-car-key_1599711.htm

https://www.freepik.com/free-vector/flat-hand-holding-house-key-background_1580865.htm

https://www.freepik.com/free-vector/group-speech-bubbles_5825567.htm

https://www.freepik.com/free-vector/hanging-photo-frames-different-sizes_13197741.htm

https://www.freepik.com/free-vector/key-business-concept-with-flat-design_2487349.htm

https://www.freepik.com/premium-vector/businessman-body-parts-elements-character-set_6640702.htm

https://www.freepik.com/premium-vector/businessman-body-parts-elements-character-set_6640703.htm

https://www.freepik.com/premium-vector/stylized-map-united-states-america-isometric-3d-green-map-with-cities-borders-capital-washington-regions_13306494.htm

https://www.freepik.com/premium-vector/browser-window-mockup-modern-internet-page_11042276.htm

https://www.freepik.com/premium-vector/corona-virus-lock-down-symbol-corona-virus-pandemic-puts-countries-lock-down-lock-down-concept-virus-outbreak_7375204.htm

https://www.freepik.com/free-vector/different-kinds-transportations_1175922.htm

https://www.freepik.com/free-vector/colorful-parachute-carrying-gift-boxes-light-blue-sky-background_10600411.htm

https://www.freepik.com/free-vector/hiring-new-people-finding-new-staff-work_25968399.htm

https://www.freepik.com/free-vector/white-house-illustration-flat-design_12418413.htm

https://www.freepik.com/premium-vector/different-actions-scenes-with-cartoon-bandit_4085279.htm

https://www.freepik.com/free-vector/camping-area-landscape_9906118.htm

https://www.freepik.com/premium-vector/mascot-character-design-bandit_4085278.htm

https://www.freepik.com/free-vector/aquarium-essential-elements-collection_4321774.htm

https://www.freepik.com/premium-vector/hand-open-drinking-tap-water-drink-falling-drop-liquid-palm-vector-illustration-flat-design-isolated-white-background-turn-turn-off-faucet-saving-water_23544313.htm

https://www.freepik.com/premium-vector/speed-optimize-load-website-page-cell-phone-mobile-cellphone-display-with-performance_27039985.htm

https://www.freepik.com/free-vector/fisherman_2869910.htm

https://www.freepik.com/free-vector/set-six-fish_2091508.htm

https://www.freepik.com/free-vector/dollars-illustration-set_6974879.htm

https://www.freepik.com/free-vector/finger-pressing-start-button_2947385.htm

https://www.freepik.com/free-vector/illustration-computer-icon_2606079.htm

https://www.freepik.com/premium-vector/cartoon-businessman-creation-kit-business-woman-man-managers-constructor-body-gesture-hairstyle-emotions-vector-set-illustration-character-man-kit-creation-set-body_16302727.htm

https://www.freepik.com/free-vector/total-control-businessman-puppet-string-authority-marionette-leadership-manager-people-doll-worker_10701207.htm

https://www.freepik.com/premium-vector/hand-hold-scissors-flat-illustration_6789534.htm

https://www.freepik.com/premium-vector/calendar-icon-december-2023-31-day-raised-page-calendar-3d-vector-illustration_26233441.htm

https://www.freepik.com/premium-vector/laptop-computer-qwerty-keyboard-with-black-key-buttons-simple-flat-vector-illustration-isolated-white-background_16597558.htm

https://www.freepik.com/premium-vector/north-america-s-indian-tent-isolated-illustration-white-background_21093154.htm

https://www.freepik.com/free-vector/red-car-white-background_4124640.htm

https://www.freepik.com/free-vector/map_3980051.htm

https://www.freepik.com/premium-vector/satisfaction-meters-scale-set_3766294.htm

https://www.freepik.com/premium-vector/resumes-cv-application-selecting-staff-resume-template-web-landing-page-banner-presentation-social-media-analyzing-personnel-resume-recruitment-concept-human-resources-management_17743748.htm

https://www.freepik.com/free-vector/happy-small-dog-set-cute-funny-puppy-practicing-different-activities-hunting-playing-eating-sleeping_11235563.htm

https://www.freepik.com/premium-vector/password-security-access-push-notice-laptop-computer_7584432.htm

https://www.freepik.com/premium-vector/set-zippers_7149760.htm

https://www.freepik.com/premium-vector/clock-illustration-icon_6721735.htm

https://www.freepik.com/premium-vector/human-hand-presses-button-entering-security-system-code-combination-pin-code-keypad-password-house-alarm-digital-combination-lock-wall-vector-illustration-flat-design_24429044.htm

https://www.freepik.com/premium-vector/students-classroom-teacher-near-blackboard-auditorium-teaches-maths-lesson-children-study-subject-kids-group-studying-elementary-primary-school-class-interior-cartoon-vector-flat-concept_19960121.htm

https://www.freepik.com/free-vector/brick-wall-abstract-background_891078.htm

https://www.freepik.com/free-vector/brick-wall-abstract-background_891078.htm

https://www.freepik.com/premium-vector/black-brick-wall-seamless-pattern_22437462.htm

Lydeffekter er hentet fra Hooksounds.com under en Premium licens eller fra pixabay.com.