VÆRKTØJ

DIALOGVÆRKTØJ

FORBEREDELSE

En detaljeret vejledning til at understøtte dialogen med dine kunder omkring sikkerhed

INDUSTRIENS FOND

ALEXANDRA INSTITUTTET

FORFATTERE

Michael Rømer Bennike, Alexandra Instituttet

Zaruhi Aslanyan, Alexandra Instituttet

Dialogværktøjet er udviklet i regi af Sb3D-projektet i samarbejde med følgende virksomheder:

Partnerne i Sb3D-projektet.
Projektet er støttet af Industriens Fond:

Indholdsfortegnelse

Om dokumentet *Forberedelse*

Dette dokument er en del af *Dialogværktøjet* sammen med *Præsentation* og *Tjekliste*.

Dokumentet indeholder en række spørgsmål, der kan bruges til at understøtte dialogen mellem flere parter om udvikling af sikker software. Hvert spørgsmål ledsages af en tilhørende vejledning, der sætter spørgsmålet ind i en større sammenhæng. Heri beskrives en række sikkerhedstemaer inden for softwareudvikling, både dem, der vedrører selve udviklingsprocessen og dem, der handler om de sikkerhedsfunktioner, som softwaren skal indeholde.

Dokumentet *Forberedelse* kan bruges af softwareudvikler-teamet til at involvere kunden, der har bestilt softwaren, i diskussionen om, hvad kravene til sikkerhed er.

Indledning

Nedenstående dialogspørgsmål tager udgangspunkt i OWASP SAMM-modellen. Da modellen er beregnet til modenhedsvurdering internt (og ikke til kunde-/udvikler-dialog), har vi udvalgt relevante spørgsmål og tilrettet dem, så de bedre understøtter dialogen. Det er de spørgsmål, der vedrører omkostningerne ved softwareudvikling og bør afklares mellem kunde og udvikler. Vi foreslår, at udvikler og kunde holder et møde, der specifikt handler om sikkerheden, hvor spørgsmålene nedenfor gennemgås:

Hvert spørgsmål er struktureret således:

a. **Spørgsmål**
b. **Motivation**
   Hvorfor er det vigtigt at få svar på dette spørgsmål?
c. **Udfordringer**
   Hvorfor kan det være svært at svare på dette spørgsmål, og hvad skal man være opmærksom på?
d. **Vejledning**
   Hvordan kan man forstå, tolke og diskutere spørgsmålet?
e. **Hvordan behandles eventuelle flertydige svar?**
   Når der ikke kan svares ubetinget ja eller nej, kan dette afsnit hjælpe med at nå til enighed. Afsnittet er ikke nødvendigvis lige relevant for alle spørgsmål.

Dialogspørgsmål

1. KRAV FRA TREDJEPART

Kilde: https://owaspsamm.org/model/governance/policy-and-compliance/

a. Spørgsmål
Hvilke eksterne regulativer skal løsningen overholde? (Hvad er f.eks. kravene til datahåndtering, datalagring m.m.?).

b. Motivation
Ved at få afdækket, hvilke eksterne krav der skal overholdes, sikrer I, at jeres virksomhed følger alle gældende love og regler. Desuden bør interne sikkerhedspolitikker være overensstemt med de aktuelle eksterne krav.
Det er vigtigt både at være bekendt med gældende eksterne krav og at overholde dem. Manglende overholdelse af love og regulativer (*compliance*) kan resultere i bøder, tab af anseelse, datalæk osv.

c. Udfordringer
Mens det ikke er til diskussion, at gældende lovgivning skal overholdes, er det stadig et fortolkningsspørgsmål, hvordan man vil sikre compliance. Det er derfor meget vigtigt, at begge parter har en fælles forståelse af, hvilke regler der er gældende.
Compliance kommer til at have stor indvirkning på prisen. Det skyldes især, at der ud over de høje krav om at være compliant, er tilsvarende høje dokumentationskrav/bevisbyrde. Der kan derfor være behov for ekstern auditering og certificering.

d. Vejledning
Læg ud med at finde ud af, hvilke love og regler som løsningen er underlagt. Det kan være, I skal søge juridisk bistand eller hente input hos jeres egne compliance-medarbejdere. I kan f.eks. overveje, hvilken datatype der anvendes eller lagres, hvor virksomheden er placeret geografisk, så der evt. gælder særlige landespecifikke regler osv. Dette trin kan gennemføres på forhånd.

e. Håndtering af flertydige svar
Det er stadig et fortolkningsspørgsmål, hvordan man skal efterleve de mange love og regulativer. Hvis man er i tvivl, bør man altid søge juridisk bistand. Hvis det er svært at nå til enighed, bør man altid tilstræbe at tolke ud fra *best practice* eller standarder for den pågældende branche, som vil blive harmoniseret med lovgivningen.

2. INTERNE SIKKERHEDSKRAV

Kilde: https://owaspsamm.org/model/governance/policy-and-compliance/

a. Spørgsmål
Hvad er de interne krav til softwaresikkerhed i organisationen?
Er disse sikkerhedskrav afstemt med kravene til compliance, jf. tidligere spørgsmål?

b. Motivation
Virksomhedens egne sikkerhedskrav (eller en sikkerhedspolitik for software) fastlægger en minimumstandard, som alle applikationer i virksomheden skal leve op til. På den måde bliver compliance-dokumentation og sikkerheds-management mere ensartet på tværs af applikationens økosystem.

c. Udfordringer
En virksomhedspolitik er normalt afstemt med (eller en fortolkning af) eksterne krav. Dog kan der afviges fra kravene i en intern politik – ofte af budgetmæssige årsager. Desuden kræver det en vis modenhed og overblik at implementere og håndhæve en sikkerhedspolitik. Derfor har virksomheder ikke altid formelle interne retningslinjer og politikker, der uden videre kan anvendes på et nyt softwaredesign. Det gælder for alle politikker, at det kan fortolkes, hvordan de skal efterleves, og det er også almindeligt med undtagelser, hvis det ikke er strengt nødvendigt at overholde en politik. Det kan være vanskeligt at afvige fra lovgivningsmæssige krav, hvorimod der kan slækkes lidt mere på de interne politikker, forudsat afvigelserne kan godkendes af den øverste ledelse.

d. Vejledning
Forberedelserne til dette trin kan gennemføres på forhånd: Kunden bør tjekke med sin egen interne sikkerhedsansvarlige, om der er en sikkerhedspolitik for softwareudvikling og de applikationer, der sættes i produktion. Enten før eller under mødet skal denne politik gennemgås grundigt ift. den pågældende software. Dette skal gerne munde ud i en liste over specifikke sikkerhedskrav, der 'ikke er til forhandling', og som er afstemt med både interne politikker og eksterne/lovgivningsmæssige krav.
Hvis der ikke findes politikker/krav, skal den fremtidige ejer af softwaren forventningsafstemme med organisationens sikkerhedsansvarlige.
Det anbefales, at man i dette trin aftaler at udvikle softwaren efter principperne for Security by Design.

e. Håndtering af flertydige svar
Som under 1.e: Hvis det er svært at nå til enighed, bør man altid tilstræbe at tolke ud fra *best practice* eller standarder for den pågældende branche, som vil blive harmoniseret med lovgivningen. Ejeren af sikkerhedspolitikken skal kunne gøre rede for, om det er passende med en fortolkning.

3. RISIKOPROFIL

Kilde: https://owaspsamm.org/model/design/threat-assessment/stream-a/

a. Spørgsmål
Har begge parter en fælles forståelse af applikationens risikoprofil? Det vil sige: er parterne enige om betydningen af at beskytte applikationen mod kompromittering, afhængig af hvor følsom applikationen er, og hvor udsat den er?

b. Motivation
Det kan være vanskeligt at afgøre, hvad der er et passende niveau af sikkerhed for en applikation. Det er derfor yderst vigtigt at nå til enighed om den overordnede risikoprofil for applikationen – dvs. hvad er de forretningsmæssige risici, hvis applikationen bliver kompromitteret – således at udvikler og kunde kan afstemme forventningerne. En risikovurdering der tager højde for det forretningsmæssige aspekt hjælper både kunden og udvikleren med at træde et skridt tilbage fra selve applikationen og se den i et bredere perspektiv. På den måde hjælper risikovurderingen med at forstå og prioritere forretningsmæssige sikkerhedskrav, som bør afspejles i sikkerhedsbudgettet og risikovilligheden.

c. Udfordringer
Det kan være meget omstændeligt at gennemføre risikovurderinger, og en detaljeret vurdering er ikke brugbar i alle typer af projekter – især ikke på et tidligt stadie. Det er dog vigtigt at få en generel forståelse af applikationens overordnede risikoniveau og indvirkning på forretningen.

d. Vejledning
Risikovurderingen behøver ikke være komplet på dette stadie. Målet er at udføre vurderingen på et meget overordnet niveau og fokusere på forretningsmæssige risici. Konkrete sårbarheder og trusler mod applikationen adresseres i det næste spørgsmål.
Hvis kunden allerede har en fremgangsmåde eller en standard for risikovurdering, kan denne anvendes. Det sikrer, at resultaterne er sammenlignelige med resten af kundens IT-økosystem, hvilket igen hjælper med at prioritere ressourcerne til at håndtere sikkerhedsrisici. Hvis der ikke er et officielt rammeværk i kundens virksomhed, kan udvikleren præsentere sin egen.
Hvis ingen af parterne har et rammeværk til risikovurdering, kan nedenstående vejledning følges: Hvis I rangerer resultatet af hvert spørgsmål på en skala fra 1–5, hvor 5 er høj risiko, og 1 er lav risiko, kan gennemsnittet heraf bruges som en rettesnor (i denne øvelse) for den forretningskritiske risiko. Her er et udvalg af spørgsmål til evaluering af den overordnede risiko for en applikation:

- **a.** Fortrolighed: Hvor følsomt er den data, som applikationen får adgang til? Er det f.eks. meget følsomt data, intellektuel ejendom, forretningshemmeligheder, personhenførbart data m.m.?
- **b.** Hvad er kravene til tilgængelighed for applikationen?
- **c.** Eksponering: Er applikationen internetvendt eller udelukkende intern?
- **d.** Eksponering: Er applikationen stand-alone, eller skal den integreres med et større økosystem? Dvs. kan en kompromittering af applikationen føre til kompromittering af andre dele af infrastrukturen?
- **e.** Host: Hvem hoster applikationen, og – hvis det er en tredjepart – er dennes sikkerhed blevet vurderet, og er der indgået SLA'er?
- **f.** Kompromittering: Hvis applikationen kompromitteres, kan det så medføre overtrædelse af lovgivningen og dermed bøder?
- **g.** Kompromittering: Kan organisationens omdømme lide skade, hvis applikationen eller data bliver kompromitteret?
- **h.** Kompromittering: Hvilke konsekvenser har det for brugerne af applikationen, hvis den bliver kompromitteret?

e. Håndtering af flertydige svar

Det er notorisk vanskeligt at lave præcise risikovurderinger, eftersom der altid vil være undtagelser, bias og formodninger, der påvirker vurderingen. I må leve med, at det kan være meget svært at få et endeligt svar på vurderingen, så forsøg i stedet at rangere risiciene. F.eks. kan I rangere økonomisk tab på en skala fra X-Y og ikke 'falde i' og begynde at diskutere, om en given risikos økonomiske tab er præcis 'X' eller 'Y' – alt er estimater. Vælg en skala til vurdering af risiciene, som er finmasket nok til at rangere og sammenligne risici men ikke så fintmasket, at I fortaber jer i detaljer. Eksempel: på en skala med mange trin fra 1 til 100, gør en risiko vurderet til 56 eller 57 ikke den store forskel, og en skala med færre trin som 'lav', 'medium' og 'høj' er måske for simpel til at sammenligne og prioritere risici. Noget derimellem som f.eks. en skala på 1-5 eller 1-10 vil passe til mange scenarier.

4. TRUSSELSVURDERING

Kilde: https://owaspsamm.org/model/design/threat-assessment/stream-b/

a. Spørgsmål
Har begge parter en fælles forståelse af risici og/eller trusler?
Har den pågældende software været igennem en risikovurdering, trusselsmodellering eller noget tilsvarende?

b. Motivation
Trusselsmodellering er en proces, der hjælper en organisation med at afdække sikkerhedstrusler og potentielle sårbarheder, prioritere dem og diskutere mulige modforanstaltninger. Desuden er det en systematisk måde at analysere og evaluere trusler og modforanstaltninger og til at identificere sikkerhedskrav.
Processen kan bruges til at få et overordnet billede af trusselslandskabet for applikationen.
Processen sikrer også, at man får et fælles sprog og en fælles forståelse af sårbarhederne.

c. Udfordringer
Trusselsmodellering kan gennemføres mere eller mindre dybdegående: fra at skabe et overordnet overblik til at afdække truslerne i detaljer. I dette trin bør fokus være på at få et overordnet billede af truslerne og ikke så mange detaljer.

d. Vejledning
Hvis der allerede findes en trusselsmodel, så brug den til at indlede diskussionen. I kan evt. overveje at udarbejde en risikovurdering/trusselsmodel af softwaren i fællesskab.
Hvis der ikke findes en trusselsmodel, kan I gennemføre en overordnet trusselsmodellering. Det kan være godt at se på eksisterende diagrammer, såsom systemdiagrammer, dataflowdiagrammer osv. I kan derefter foretage en brainstorm ved et whiteboard eller med pen og papir.

Der findes mange trusselsmodelleringsteknikker. I kan vælge den teknik, der passer bedst til jer, da der ikke er en generelt accepteret industristandard for trusselsmodelleringsprocessen. De fleste modelleringsteknikker omfatter oftest disse tre trin: systemmodellering, trusselsafdækning og risikorespons i en eller anden form. Hvert af disse trin kan tilgås på forskellig vis og med forskellige detaljeringsgrader.

Disse tre spørgsmål kan hjælpe med at skabe struktur i trusselsmodelleringen, og de hænger sammen med de tre trin nævnt ovenfor:

- Hvad har vi med at gøre? (systemmodellering)
- Hvad kan gå galt? (afdækning af trusler)
- Hvad vil vi gøre ved det? (risikorespons)

e. Håndtering af flertydige svar
Der kan nemt være flertydige svar i dette afsnit, så brug vejledningen ovenfor til at mindske uklarhederne mest muligt.

5. FUNKTIONELLE SIKKERHEDSKRAV

Kilde: https://owaspsamm.org/model/design/security-requirements/

a. Spørgsmål

Findes der en specifikation over sikkerhedskrav?

a. Er sikkerhedskravene afstemt med kravene i spørgsmålene under *Interne sikkerhedskrav*?
b. Er sikkerhedskravene afstemt med resultaterne af risiko- og trusselsvurderingen? Dvs. er der for hver fundet trussel/risiko, som overskrider det acceptable niveau, tilsvarende foranstaltninger til at afhjælpe risikoen?
c. Er sikkerhedskravene afstemt med officielle baselines, rammeværk eller standarder for sikkerhed?

b. **Motivation**

Denne aktivitet har til formål at sikre, at der er en forståelse af de vigtigste sikkerhedskrav under udviklingsprocessen. Desuden skal forventningerne til sikkerhed afstemmes med resultaterne fra spørgsmålene under *Interne sikkerhedskrav* samt eventuelle risiko- og trusselsvurderinger.

c. **Udfordringer**

Det er ikke let at udpege og beskrive alle sikkerhedskrav i detaljer. Men selv sikkerhedskrav, der er udformet på et overordnet niveau, kan være en stor hjælp til at få udviklet passende sikkerhedsforanstaltninger. Forsøg at gøre sikkerhedskravene så præcise og målbare som muligt, så de er lettere at nå til enighed om.
Sørg for at prioritere sikkerhedskravene, og del dem op i *need-to-have* og *nice-to-have*, så I kan få en snak om, hvor I skal trække grænsen.

d. Vejledning

Tag udgangspunkt i de funktionelle krav og kundens problemstillinger, når sikkerhedskravene udarbejdes. Kravene skal være så præcise og målbare som muligt og være afstemt med de interne politikker og eksterne regulativer.
Gennemgå de funktionelle krav til applikationen for at få klarlagt relevante sikkerhedskrav (dvs. forventninger) til hver funktionalitet. Gennemgangen skal tage udgangspunkt i det ønskede niveau af informationssikkerhed for applikation og data, dvs. *fortrolighed*, *integritet* og *tilgængelighed*.
Kravene skal beskrive *formålet* (f.eks. ”persondata til registreringsprocessen skal overføres og gemmes sikkert”) men ikke *løsningen* (f.eks. ”brug TLSv1.2 til sikker overførsel”).
Pas på ikke at tilføje krav, der er for generelle til at være anvendelige for den pågældende applikation (f.eks. ”applikationen skal være beskyttet iht. OWASP Top 10”). Selv om det jo er korrekt, hjælper det ikke med at blive særlig konkret.

e. Håndtering af flertydige svar

Dette spørgsmål skulle ikke give anledning til så mange flertydige svar. Resultatet bliver en liste over funktionelle sikkerhedskrav, som selvfølgelig kan være subjektive og flertydige, men eftersom spørgsmålet ikke handler om at finde løsninger til kravene, skulle det være ret ligetil at blive enige om selve kravene.

6. SIKKERHEDSARKITEKTUR

Kilde: https://owaspsamm.org/model/design/security-architecture/

a. Spørgsmål

Har begge parter en fælles forståelse af deres respektive roller i udviklingen af løsningens sikkerhedsarkitektur?
Er der valgt særlige rammer eller standarder, der skal drive softwareudviklingen?
Underspørgsmål:

- Er kunden involveret i udviklingsprocessen omkring sikkerhedsarkitekturen?
- Er kunden involveret i review- og testprocessen?
- Er kundens eksisterende sikkerhedspolitikker og guidelines indtænkt i sikkerhedsarkitekturen – eller burde de være det?

b. Motivation

Sikkerhedsarkitektur er et sæt værktøjer, rammeværk og sikkerhedsprincipper, som danner rammen for udvikling og implementering af sikkerhedsforanstaltninger og -politikker, der skal beskytte et produkt mod cybertrusler. Med en sikkerhedsarkitektur omsættes forretningskrav til eksekverbare sikkerhedskrav.
For at få et sikkert produkt, er det nødvendigt med en stærk sikkerhedsarkitektur. Ved at indtænke de rette sikkerhedsforanstaltninger på et tidligt stadie, mindsker man sårbarhederne og undgår udgifterne ved at skulle håndtere dem senere. Med en stærk sikkerhedsarkitektur indarbejder man sikkerheden i alle dele af et produkts livscyklus og gør det nemmere at beslutte, hvilke teknologier der er bedst egnet, og hvornår de skal implementeres. Desuden opnår man compliance ift. relevante myndigheder og regulativer.

c. Udfordringer

Det kan være en udfordring at vælge et passende niveau af sikkerhedsarkitektur, da man kan blive ved i det uendelige. For at opnå størst mulig omkostningseffektivitet bør ambitionsniveauet for sikkerhedsarkitekturen være afstemt med risikovurderingsindsatsen for at få sat passende mål for arkitekturen, ligesom arkitekturen skal være baseret på virksomhedens risikoappetit. Hvor meget træning kræver det for eksempel, hvor meget tid skal der sættes af til validering og indarbejdelse af security by design-funktionalitet, og hvad er kompleksiteten i de rammer og standarder, man har valgt at designe arkitekturen ud fra?

d. Vejledning

Det primære formål med denne aktivitet er at blive enige om, hvor meget parterne hver især skal være involveret i udviklingsprocessen omkring sikkerhedsarkitekturen. Sørg for, at alle vigtige aktører deltager i aktiviteten. Afhængigt af hvor formelt man går til værks, kan man starte med at definere arkitekturdesignopgaver og herefter tildele roller og ansvarsområder ved hjælp af RACI-matrix m.m.
I kan også overveje at diskutere rammerne for og hovedelementerne i sikkerhedsarkitektur. Vælg et arkitekturframework som passer godt til produktet og organisationen. Læg ud med at få en grundig forståelse af produktet. Diskuter teknologier, data, brugere m.m. omkring produktet og saml viden om processer og politikker. Indtænk kundens forretningsmål/-krav, og hvordan I vil indarbejde dem i sikkerhedskravene.

e. Håndtering af flertydige svar

Formålet med dette spørgsmål er at udelukke tvetydige svar ift. roller og ansvarsfordeling i forbindelse med sikkerhedsarkitekturspørgsmålene. Når spørgsmålene er gennemgået, skal der f.eks. være entydige svar på, hvor meget hhv. kunde og udvikler skal være involveret.

7. SIKKERHEDSTEST OG IMPLEMENTERING AF LØSNING

Kilder: https://owaspsamm.org/model/verification/requirements-driven-testing/
https://owaspsamm.org/model/verification/security-testing/

a. Spørgsmål

Hvilke typer af sikkerhedstest har I brug for?
Hvilke typer af sikkerhedstest udfører I?

- Tester I, om sikkerhedskontroller fungerer korrekt?
- Gennemfører I sikkerhedstest (både manuelle og automatiserede/værktøjsbaserede)?
- Anvender I nogen former for automatiserede testværktøjer?
- Hvem er ansvarlig for hver type test?
- Gennemføres der test som en del af SDLC eller som en integreret del af en CI/CD pipeline?

b. Motivation

Sikkerhedstest handler om at validere relevante sikkerhedskontroller, dvs. at få verificeret, at standard-softwaresikkerhedskontroller virker som forventet. Desuden kan test være med til at afsløre eventuelle sårbarheder eller svagheder ved den tekniske implementering.
Sikkerhedstest sikrer, at softwaren er uden sårbarheder, der kan kompromittere funktionalitet, ydeevne eller dataintegritet. Ved at tage hånd om de fundne sårbarheder og få bekræftet, at sikkerhedskontrollerne er korrekt implementeret, reducerer man angrebsfladen.

c. Udfordringer

Der er mange udfordringer, som kan vanskeliggøre sikkerhedstest, især mangel på tid og ressourcer, komplekse scenarier og skiftende krav.
Det går ofte ud over testarbejdet, hvis det placeres i slutningen af SDLC, eftersom de sidste faser i SDLC ofte lider under forsinkelser eller budgetoverskridelser fra tidligere faser. Det er vigtigt at overveje, hvor meget softwaren løbende skal testes, så man undgår at finde alvorlige sårbarheder tæt på deadline.

d. Vejledning

Husk at jo tidligere i SDLC I tester og opdager fejl, jo billigere er det som regel at udbedre dem. Så for at undgå problemer, bør der i projektet være planlagt med løbende test og/eller modultest fordelt gennem hele SDLC. Sørg for, at kunde og udvikler har afstemt forventningerne ift. test, at der er allokeret nok tid og ressourcer til det, og vær tydelig omkring, hvad værdien og fordelene er for kunden.
For at lykkes med testprogrammet, skal I være enige om de testmål, der er fastlagt i sikkerhedskravene. Forsøg at nå til enighed om, hvordan testen bedst udføres, hvor omfattende den skal være, og om kunden skal være med til at definere sikkerhedstestcases.
Mange sikkerhedssårbarheder svære at få øje på uden at inspicere kildekoden grundigt. Overvej at bruge automatiserede testværktøjer, der kan sikre dybde og præcision i inspektionen, og hvor der tages højde for robusthed og nøjagtighed i sikkerhedstestcasene, tilgængelige integrationer med andre værktøjer, anvendelse samt omkostningsmodel.

e. Håndtering af flertydige svar

Der kan let forekomme flertydige svar i dette afsnit, så brug ovenstående vejledning til at mindske usikkerhederne mest muligt.

Afrunding og næste skridt

Når I har været igennem de 7 spørgsmål, skal I opsummere jeres svar og diskutere med kunden, hvad de næste skridt er.

Med udgangspunkt i opsummeringen, bør I i fællesskab kunne svare på følgende:

- Har I fået en fælles forståelse af sikkerhedskravene til applikationen?
- Har I fået en fælles forståelse af ansvarsfordelingen imellem jer?
- Er der sikkerhedsaspekter omkring løsningen, som I stadig mangler at gennemgå?
- Er der emner inden for de 7 spørgsmål, som I stadig mangler at nå til enighed om?

Hvis I har brug for at skabe yderligere klarhed og forståelse, skal I nu beslutte jer for, hvad der skal til for at nå til enighed, inden I afslutter mødet. For eksempel synes du eller kunden måske, at der er behov for en cost-benefit-analyse, en mere detaljeret risikovurdering eller for at rådføre sig med andre personer i jeres respektive organisationer.

Dokumentér alle jeres beslutninger og konkrete tiltag, der skal til, for at I når til enighed, så I kan følge op på det senere.