SECURITY
BY
DESIGN

SÅDAN KOMMER DU I GANG

SECURITY BY DESIGN

SbD

SECURITY
BY
DESIGN

INDUSTRIENS FOND

Indhold

Indledning

Security by design (SbD) handler om at tænke sikkerhed ind i alle faser af softwareudviklingen, så det spiller en rolle i alt fra design over implementering til vedligeholdelse. Det primære mål med SbD er at opnå større sikkerhed i slutproduktet og dermed beskytte virksomhedens forretningsmål, men SbD hjælper også med at gøre sikkerhed til en naturlig del af udviklingsprocessen. SbD er altså ikke kun en teknisk øvelse – det er også et strategisk og organisatorisk valg. Men hvad betyder det i praksis? Hvordan kan I som virksomhed gribe det an – og hvad med projekter, der allerede er i gang?

Først og fremmest: *Det er aldrig for sent at gå i gang med SbD, men det er vigtigt, at I prioriterer at komme i gang.* Det er ikke for sent at tænke sikkerhed ind i udviklingen af et produkt, der allerede har en kodebase og måske er delvist i produktion. Så længe I udvikler, kan I nå at gøre noget. Dog er det vigtigt at holde sig for øje, at arbejdet med at integrere sikkerhed i produktet bliver større, jo længere det udskydes.

I denne guide fortæller vi om principperne i SbD og peger på konkrete steder, I kan sætte ind. Guiden er delt ind i fire afsnit, hvor hver overskrift giver en tommelfingerregel til SbD.

Det første afsnit hedder 'Tal om sikkerhed' og beskriver den fase, hvor I skal afgøre, hvad sikkerhed betyder i konteksten af jeres virksomhed og produkter.

Det andet afsnit hedder 'Integrer sikkerhed i processen' og vejleder jer i, hvordan I kan gøre netop det.

Det tredje afsnit hedder 'Sikkerhed skal forankres i organisationen' og handler om at få ansvaret og opgaverne placeret de rigtige steder.

Det sidste afsnit hedder 'Afsæt ressourcer til sikkerhed' og omhandler, hvad I bør være opmærksomme på, når I afsætter ressourcer til sikkerhed.

Guiden kan læses fra ende til anden og implementeres i nævnte rækkefølge, men I kan også bruge den iterativt, hvor I ad flere omgange går til det afsnit, der er relevant for den proces, I er i gang med.

Det vigtigste i forhold til at komme godt i gang med SbD er at gå kritisk og nysgerrigt til jeres egne processer og rutiner.

Tal om sikkerhed

For at kunne arbejde effektivt med sikkerhed er det nødvendigt at have en fælles forståelse af, hvad sikkerhed konkret betyder i jeres organisation, for jeres produkter og forretningsmål.

En måde at opnå dette er ved at tale om det. Ved at have løbende samtaler om sikkerhed er det desuden sandsynligt, at I bliver opmærksomme på problemstillinger, I bør forholde jer til og handle på.

Hvordan I bedst griber samtalen om sikkerhed an, afhænger af jeres organisation, virksomhedens størrelse, jeres kultur, jeres ekspertiser mv.

I kan kickstarte processen f.eks. ved hjælp af workshops, kurser, sparring og konsultation fra udefrakommende eksperter mv.

I kan også sætte jer sammen og have en mere eller mindre uformel samtale om emnet. I kan f.eks. tage udgangspunkt I jeres produkter eller systemer og diskutere, hvilke it-sikkerhedshændelser der kan true dem, og hvilke konsekvenser det vil kunne få.

I større virksomheder kan det være en fordel at nedsætte en gruppe til at lave en intern definition af sikkerhed, som I kan tage afsæt i på tværs af organisationen. Der bør så vidt muligt indgå personer fra forskellige lag og dele af organisationen, som har forskellige baggrunde og tilgange til emnet. Når gruppen har udarbejdet en definition, er det vigtigt, at den kommunikeres ud til resten af organisationen. Det kan f.eks. ske ved hjælp af skriftlige guidelines, orienterende møder eller regelmæssig sikkerhedstræning af de ansatte.

Tænk over at gøre kommunikationen så konkret og præcis som muligt. Forsøg at gøre beskrivelsen vedkommende for hver enkelt medarbejdergruppe, så det er tydeligt, hvordan sikkerhed er relevant i forhold til deres opgaver. Dette kan f.eks. gøres ved at udfolde generiske beskrivelser og guidelines på forskellige måder for de enkelte grupper.

Integrer sikkerhed i processen

En hjørnesten i SbD er, at det ikke er tilstrækkeligt at tænke sikkerhed ind i slutningen af processen – eller for den sags skyld i starten.

Dermed ikke sagt, at I skal opgive etablerede sikkerhedsprocedurer, der er knyttet til et bestemt sted i udviklingen. I skal dog være opmærksomme på, at de ikke kan erstatte det løbende arbejde med sikkerhed i udviklingsprocessen.

BRUG EN LEDELSESSTRATEGI, DER VÆRDSÆTTER SIKKERHED

At udvikle sikre systemer og løsninger er en kontinuerlig proces. Nye angreb og sikkerhedshuller opdages hele tiden, hvilket bevirker, at systemer, der tidligere blev betragtet som sikre, pludselig kan ophøre med at være det.

Derudover kan løsninger, vi anser for at være sikre i dag, ikke nødvendigvis betragtes som værende sikre i morgen, fordi reguleringer og forventninger til sikkerhed er i konstant forandring. Sikkerheden af jeres produkt har derfor brug for tilbagevendende opmærksomhed og en ledelsesstil, der understøtter den.

Enhver ny hændelse – hvadenten det er en ny feature, en bug eller opdagelsen af en sårbarhed – skal evalueres og vurderes, før produktet sættes i produktion. Når et produkt er i produktion, skal der være procedurer på plads, der sikrer, at det er let at rapportere, følge op på og reagere på nye sårbarheder.

SKITSER SYSTEMET

Vedligehold et opdateret overblik over jeres system og de trusler, der er mod det. Det er centralt for SbD at have et overbliksbillede af systemet, hvilket ofte omtales som en model af systemet. Modellen viser det overordnede design af systemet uden for mange detaljer.

En simpel model kan laves som en tegning på en tavle, men der kan også anvendes mere eller mindre avancerede værktøjer.

Modellen kan bruges til at starte uformelle samtaler om sikkerhed med medarbejdere, men dens primære formål er at give jer mulighed for at opdage og undersøge angrebsvinkler, der ikke er umiddelbart iøjnefaldende, og gøre jer opmærksomme på potentielle sikkerhedsproblematikker, før de bliver problematiske. Modellen hjælper således med at finde trusler mod systemet.

At finde og analysere mulige trusler omtales til tider som *trusselsmodellering*. Dette kan gøres manuelt ved brug af simple værktøjer (som f.eks. OWASP Threat Dragon eller Microsoft Threat Modelling Tool) eller ved at bruge modellen af systemet som input til mere avanceret software, der

automatisk kan identificere og vurdere mulige angreb og trusler. Sker der noget nyt – det kan f.eks. være, at I har udviklet en række features eller opdaget nye bugs eller sårbarheder – så opdateres modellerne.

VÆR EKSPLICIT OMKRING RISICI

Alle trusler skal enten imødegås, eller også skal de risici, der er forbundet med dem, accepteres. Når en liste af trusler er blevet identificeret, er det vigtigt at adressere dem alle. For at vurdere de risici, der er forbundet med en trussel, inddrages både konsekvenserne af et angreb, og hvor sandsynligt det er, at det vil ske. Nogle risici kan accepteres, som de er, andre skal imødegås.

At acceptere risici kan have store konsekvenser for jeres virksomhed, kunder og forretningspartnere. Når I vælger at acceptere en risiko, bør det derfor altid være en forretningsbeslutning.

INTEGRER SIKKERHEDSSPØRGSMÅLET I JERES ARBEJDSPROCES

Organisatorisk er det vigtigt, at sikkerhedsspørgsmålet bliver integreret i jeres arbejdsgange hele vejen fra ledelsen og ned i de enkelte teams. Det kan I f.eks. gøre ved at lade sikkerhedsspørgsmålet og opdatering af modellen være en fast del af jeres SCRUM-cyklus, eller ved at det indgår som en del af tjeklister til kodereviews.

BRUG DE RIGTIGE VÆRKTØJER OG TEKNIKKER, OG AUTOMATISER HVOR DET ER MULIGT

Sikkerhed er svært, og uanset hvor dygtige medarbejdere I har ansat, er det vigtigt at understøtte deres arbejde med relevante værktøjer. Et sted, hvor det kan være gavnligt at anvende værktøjer, er f.eks. til software-verificering.

Man kan verificere et stykke software på mange niveauer:

- man kan få en anden udvikler til at bedømme det (review),
- man kan teste det,
- man kan bruge statiske værktøjer som f.eks. en linter[1] til at analysere det,
- man kan skrive i et sprog, der ikke tillader, at man skriver (visse typer af) forkert kode.

På hvert niveau findes der værktøjer, der kan hjælpe med at automatisere noget af processen. Det skal dog nævnes, at disse værktøjer generelt ikke er gratis; de koster både tid og penge at bruge. Men de rette værktøjer kan tjene sig selv hjem igen i form af hurtigere udvikling og færre fejl.

Et par vigtige teknikker, der hjælper med at forbedre sikkerheden, er trussels- og risikovurdering. I en trusselsvurdering forholder I jer til, hvilke sikkerhedshændelser det er mest sandsynligt, at jeres virksomhed og produkter kommer ud for. Risikovurderingen giver overblik over systemet og hjælper jer med at finde trusler og relaterede risici. Derudover hjælper den også med at undersøge, om allerede eksisterende sikkerhedsforanstaltninger er tilstrækkelige, eller om det er nødvendigt at foretage flere.

1 *En linter er et statisk analyseværktøj, der hjælper med at finde visse typer af fejl i koden, mens den skrives.*

Sikkerhed skal forankres i organisationen

Arbejdet med sikkerhed skal forankres i organisationen. Er sikkerhed ikke tydeligt forankret i virksomheden og betragtes som et fælles ansvar, vil den enkelte medarbejder være tilbøjelig til at tænke: *"Det er der nok nogen andre, der tager sig af."*

Forankringen kan ske gennem uddelegering og formalisering af ansvar, men det kan også ske processuelt gennem faste rutiner, procedurer, tjeklister mv. Præcis hvordan forankringen sker bedst, afhænger af den enkelte organisation.

I mindre virksomheder kan det f.eks. være nødvendigt at placere hovedansvaret hos en enkelt udvikler eller projektleder. I en større organisation bør være muligt at forankre sikkerheden på alle niveauer. Der kan f.eks. udpeges en sikkerhedsambassadør på hvert hierarkisk trin.

Når ansvaret placeres hos enkeltpersoner, bør man være opmærksom på den skrøbelighed, denne konstruktion medfører. Hvad sker der f.eks., hvis medarbejderen skifter arbejde eller går på pension? Derudover er sikkerhed et stort område, som det kan være uoverskueligt for en enkelt medarbejder at have overblik over og holde sig opdateret på. Det er desuden vigtigt, at alle medarbejdere ved, hvor de kan gå hen med spørgsmål, overvejelser, bekymringer mv. vedrørende sikkerhed.

Sikkerhed skal forankres i ledelsen, uanset organisationens størrelse. At ledelsen prioriterer sikkerhed, legitimerer, at det fylder andre steder i processen. Det er ikke nogens hobby- eller sideprojekt men en vigtig del af udviklingen.

At forankre sikkerhed i ledelsen kan gøres på forskellige måder som f.eks.:

- at ledelsen definerer sikkerhedsparametre, som der skal afrapporteres i forhold til,
- at det gøres til et forretningsmål i sig selv at udvikle sikre produkter,
- at repræsentanter fra ledelsen deltager i virksomhedens security board og/eller i gennemførelsen af f.eks. risikovurderinger.

DOKUMENTER INDSATSEN

At dokumentere indsatsen på sikkerhedsområdet kan medvirke til at gøre indsatsen mere robust, f.eks. overfor skift i medarbejderstaben. Det hjælper også med at gøre processen mere transparent og kan give den enkelte medarbejder et bedre overblik. Dette kan desuden give andre medarbejdere øget mulighed for at bidrage til processen.

SIKKERHED GÆLDER OGSÅ FOR PRODUKTER, DER ER I PRODUKTION

Arbejdet med sikkerhed stopper sjældent i det øjeblik, et produkt sættes i produktion. Det er derfor vigtigt, at denne del af arbejdet også forankres i organisationen, og at ansvarsfordelingen er klar og utvetydig.

Vær opmærksom på, at sikkerheden omkring produkter, der er i produktion, ikke nødvendigvis varetages af de samme personer og mekanismer, som havde ansvaret under udviklingen.

Afsæt ressourcer til sikkerhed

Der ligger to aspekter i prioriteringen af ressourcer til sikkerhed: Dels handler det om, at ressourcerne bliver afsat, dels skal ressourcerne bruges på den bedste måde.

Det er vigtigt, at I afsætter ressourcer til at arbejde målrettet med sikkerhed. Da sikkerhed ikke kan håndteres én gang for alle på et bestemt tidspunkt i processen, er det nødvendigt at afsætte ressourcer til sikkerhed gennem hele udviklingsforløbet.

Det er vigtigt at bruge de allokerede ressourcer på den mest effektive måde, så I fokuserer på de områder, hvor I får mest mulig sikkerhed for pengene. Til at vurdere hvordan I gør dette, kan det være en hjælp at lave en risiko- eller trusselsvurdering.

Hvad så nu?

Sikkerhed indføres ikke i en håndevending; det gør SbD desværre heller ikke. SbD er en proces og kan implementeres lidt ad gangen eller i store skridt.

SbD starter i toppen af en organisation, så det første skridt er at blive enige med ledelsen om, at SbD er en god idé for jeres virksomhed. Dernæst skal I blive enige om, hvad sikkerhed betyder for jer.

Med andre ord: tal om sikkerhed – også med ledelsen.

Derudover er SbD en iterativ proces. I behøver altså ikke være helt færdige med et punkt, før I går videre til det næste; I kan komme tilbage til punktet på et senere tidspunkt.

Denne guide er tænkt som en hjælp til at komme i gang med SbD.

Du kan finde mere information om SbD på: securitybydesign.alexandra.dk

KONTAKT

ALEXANDRA INSTITUTTET
Sebastian Holmgaard Christophersen
E-mail: s.christophersen@alexandra.dk
Telefon: +45 93 52 26 54

PROJEKTPARTNERE

DECEMBER 2022

Sb3D er et samarbejde mellem DTU Compute, Institut for Datalogi på Aalborg Universitet, Dansk Erhverv, Dansk Industri, Erhvervshus Midtjylland og Alexandra Instituttet. Projektet er finansieret af Industriens Fond.