BrightFlow beveiligingsbeleid

Beveiliging bij BrightFlow speelt vanaf de ontwerpfase van maatwerksoftware een belangrijke rol. Samen met schaalbaarheid vormt het de basis van onze softwarearchitectuur. In IT-jargon wordt dit 'security by design' genoemd. Aan de hand van de belangrijkste aandachtspunten leggen wij uit wat jouw voordelen zijn van deze ontwikkelingsfilosofie en wat het je als opdrachtgever oplevert.

1. Veiligheid als ontwerpprincipe

Zoals de term al doet vermoeden betekent ‘security by design’ dat wij beveiliging in elke fase van de ontwikkeling hanteren als uitgangspunt. Dit begint bij de softwarearchitectuur. Voor het ontwerp van de architectuur gaan we na welke maatregelen nodig zijn om te voldoen aan de beveiligingseisen. Denk bijvoorbeeld aan het inbouwen van een autorisatie- en authenticatieproces en het gebruik van encryptie.

2. Cryptografie

Een belangrijk onderdeel van security by design is cryptografie. Dit is een techniek om informatie te coderen en decoderen. Hierdoor kunnen alleen de gewenste personen de informatie gebruiken en het beschermt de data tegen onbedoelde toegang. Ook kan het helpen bij de multi-factor authenticatie en autorisatie van gebruikers. Zo kan je beveiligde toegang verlenen aan specifieke gebruikers en het versterkt de beveiliging van de data.

3. Toegangsbeheer

Ook maken we afspraken over toegangsrechten en over welke data waar opgeslagen mag worden. Het waarborgt de veiligheid van de informatie door duidelijke afspraken te maken over wie toegang heeft tot welke data en functies. Zo voorkomen we dat er onbedoeld gevoelige informatie buiten de juiste context terechtkomt. Dit gebeurt bijvoorbeeld door het toewijzen van specifieke rechten aan gebruikers of rollen, en zorgt voor een efficiënte en veilige manier van informatie delen. Toegangsbeheer is een belangrijke stap in security by design, die ervoor zorgt dat de informatie alleen toegankelijk is voor de juiste personen.

4. Codebeveiliging

De beveiliging van de softwarecode is net zo belangrijk als de beveiliging van de data. Tijdens het programmeren houden we rekening met de beveiligingsrichtlijnen en monitoren we de code continu op mogelijke risico's. Hierdoor voorkomen we dat er kwetsbare plekken in de code ontstaan. Ook ontwikkelen wij met het meest gerenommeerde ontwikkelingsplatform ter wereld. Als er een veiligheidsrisico is, kunnen we rekenen op een adequate reactie van de leverancier die het probleem oplost. Bovendien zijn we verzekerd van de continue ontwikkeling van software-updates die bedreigingen neutraliseren. Jouw maatwerksoftware is hierdoor optimaal beveiligd en altijd up-to-date.
Daarnaast versterken we de codebeveiliging via code-reviews en het gebruik van beveiligingstools. Hierdoor kan jij als onze opdrachtgever er zeker van zijn dat er op verschillende manieren wordt gewerkt aan de beveiliging van de softwarecode.

5. Up-to-date

Net als onze softwareleveranciers en serviceproviders, nemen wij ook onze verantwoordelijkheid serieus om de gebruikte tools en onze infrastructuur veilig te houden. Dit betekent dat we werken met de meest recente versies van onze tools en extensies. Deze testen we vooraf grondig alvorens ze in gebruik te nemen. Bovendien houden we onze infrastructuur up-to-date en maken we gebruik van versleutelde verbindingen. Hierdoor kunnen we snel reageren en maatregelen nemen om de beveiliging van onze applicaties en servers te waarborgen. Tevens voeren we regelmatig beveiligingsanalyses uit om de beveiliging van de software van onze klanten te versterken.

6. Responsible disclosure

Daarnaast hanteren wij het zogenaamde responsible disclosure beleid. Dit betekent dat wij onder specifieke voorwaarden ons beleidsmatig openstellen voor de veiligheidstests van ethische hackers. In het geval dat er onverhoopt een kwetsbaarheid in één van onze applicaties aan het licht komt, biedt dit de mogelijkheid om het aan ons te melden en nemen we adequaat reageren.

7. Onderhoud

Om de veiligheid ook na oplevering te garanderen, verzorgen wij het onderhoud waarbij we de klantapplicaties en desgewenst de hostingomgeving continu monitoren. Hierdoor detecteren we proactief mogelijke beveiligingsproblemen en kunnen we direct actie ondernemen om deze op te lossen.
Beveiliging zien wij als een continu proces. Als opdrachtgever kun je erop vertrouwen dat wij alles in het werk stellen om jouw software veilig te houden, vanaf de basis tot en met het onderhoud.

IT-compliance

Als je plannen hebt om je bedrijf te certificeren volgens de ISO-normen, dan is werken met maatwerksoftware van BrightFlow een stap in de goede richting. Onze software voldoet aan de eisen van de ISO-normen. Dit maakt het behalen van certificeringen eenvoudiger en helpt bij het verbeteren van de processen van jouw bedrijf.

Meer weten?

Als je wilt weten hoe wij jouw bedrijfskritische software ontwerpen, ontwikkelen en onderhouden, neem dan contact met ons op via brightflow.nl.