

ARTIKELN | 1 APRIL 2019

ONTWIKKELEN MAATWERKSOFTWARE: RISKANTE ONDERNEMING?

Auteur: Frank Niessink

Beeld: Adobe Stock - Pixabay - Lukas

Leestijd: 6 min



ICTU heeft jarenlang ervaring met het ontwikkelen van maatwerksoftware voor verschillende overheden. Momenteel werkt ICTU samen met andere organisaties aan een praktische en risicogebaseerde richtlijn voor het borgen van de kwaliteit van maatwerksoftware. Deze richtlijn moet komend najaar leiden tot een nieuwe NEN-praktijkrichtlijn.

Het ontwikkelen van software is notoir lastig. De voorbeelden van mislukte softwareprojecten zijn legio. Toch zijn veel risico's, juist dankzij die mislukkingen, ook bekend. Bij softwareontwikkeling wordt een groot aantal risico's veroorzaakt doordat er een nieuw softwareproduct wordt gemaakt. En dat betekent per definitie dat er onwetendheid in het spel is.

Over (niet) weten

Phillip Armour betoogde al in 2000 dat softwareontwikkeling gezien moet worden als een proces van kennisverwerving en reductie van onwetendheid.¹ Softwareontwikkeling is vooral moeilijk, zo stelt hij, omdat we niet weten wat we niet weten over de software die nog ontwikkeld moet worden. Dit verklaart volgens Armour het '90%-klaarsyndroom'. Dat

AUDIT

MAGAZINE

houdt in dat een programmeur met overtuiging verklaart voor 90% klaar te zijn, soms maandenlang. Armour noemt iets niet weten onwetendheid van de eerste orde. Het niet weten wat je niet weet is onwetendheid van de tweede orde. Het laatste type onwetendheid is de bron van veel problemen bij softwareontwikkeling.



Ontdekken en voorkomen van fouten

Er zijn de nodige methoden en technieken beschikbaar die zich richten op de onwetendheid van de eerste orde. De programmeur weet niet welke fouten er gemaakt zijn bij het programmeren, maar weet wel dat er fouten zijn gemaakt. Geautomatiseerde regressietesten brengen fouten in de ontwikkelde software aan het licht voordat de software wordt geleverd aan de gebruiker.

Hetzelfde geldt voor beveiligingsproblemen. Voor vrijwel alle moderne software worden bibliotheken met generieke codes gebruikt voor bijvoorbeeld het lezen en schrijven van databases, voor grafische userinterfaces en voor het koppelen met andere systemen. Het is niet bekend welke van de gebruikte bibliotheken beveiligingsproblemen bevatten, maar de programmeur weet wel dat er altijd beveiligingsproblemen zijn die zich vroeg of laat kunnen manifesteren. Security tools, die de broncode automatisch controleren op veelvoorkomende beveiligingsproblemen, helpen potentiële beveiligingsproblemen te ontdekken vóórdat hackers er misbruik van kunnen maken.

Agile

De opkomst van zogenaamde agile-ontwikkelmethoden is gezien de risico's van onwetendheid logisch: het kortcyclisch incrementeel nieuwe versies van software opleveren is een manier om onwetendheid van de tweede orde zo snel mogelijk te verkleinen. Opdrachtgever en opdrachtnemer denken te weten welke functionaliteit gemaakt moet worden om het projectdoel te realiseren, maar pas wanneer de software in de praktijk getest of gebruikt kan worden, blijkt of de nieuwe software daadwerkelijk de functionaliteit bevat die de opdrachtgever bedoeld of gewild had.

Softwareontwikkeling is vooral moeilijk omdat we niet weten wat we niet weten

ICTU past al bijna tien jaar agile-ontwikkelmethoden toe voor het ontwikkelen van maatwerksoftware voor haar opdrachtgevers. ICTU heeft deze ontwikkelmethoden aangevuld en uitgebreid om de risico's van maatwerksoftwareontwikkeling zoveel mogelijk te verminderen. Met behulp van deze kwaliteitsaanpak heeft ICTU samen met andere overheden inmiddels enige tientallen projecten succesvol uitgevoerd. Om deze aanpak aan te vullen

met de ervaringen en geleerde lessen van andere organisaties, en deze overdraagbaar te maken en breder uit te dragen, ontwikkelt ICTU samen met andere organisaties onder de paraplu van de NEN een zogeheten Nederlandse Praktijkrichtlijn (NPR 5326) voor Kwaliteitsborging van maatwerksoftwareontwikkeling en -onderhoud, nr. 5326.

Het doel van NPR 5326 is organisaties handvatten bieden om veelvoorkomende risico's van maatwerksoftwareontwikkeling en -onderhoud te mitigeren. De NPR 5326 biedt beheersmaatregelen waarvan bekend is dat ze effectief de risico's mitigeren. Denk aan meer technische maatregelen zoals de eerdergenoemde geautomatiseerde regressietesten, maar ook aan organisatorische maatregelen zoals het ondersteunen van maatwerksoftwareprojecten en/of -teams met gespecialiseerde diensten rond beveiliging en performance.

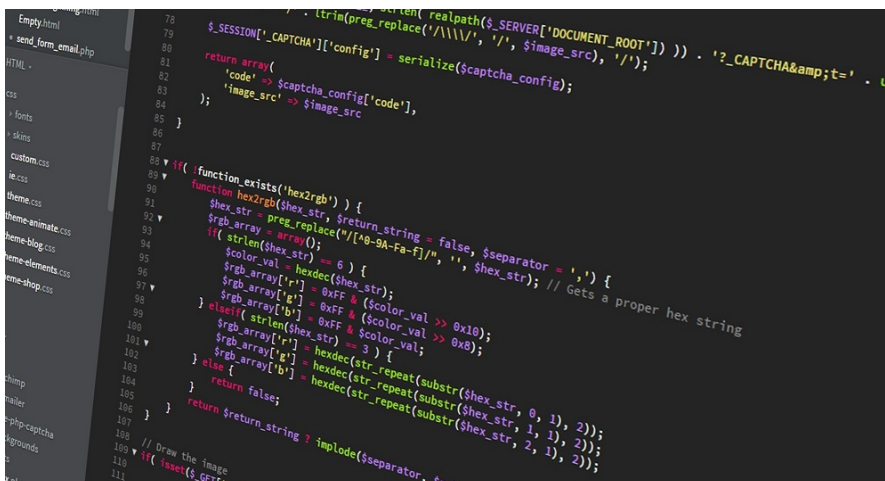
Over ICTU

ICTU is een onafhankelijke advies- en projectenorganisatie binnen de overheid. ICTU helpt overheden bij het verbeteren van hun dienstverlening met ICT, in dienst van het openbaar bestuur. Samen met opdrachtgevers realiseert ICTU kwalitatief hoogwaardige digitale dienstverlening zodat burgers en bedrijven de zaken die ze doen met de overheid veilig en makkelijk digitaal kunnen afhandelen. ICTU is in 2001 opgericht als overheidsstichting zonder winstdoel.

Risicovoorbeeld en beheersmaatregelen

Een voorbeeld van een risico is: te weinig aandacht voor het voorkomen en verhelpen van technische schuld waardoor de onderhoudbaarheid daalt. Als een opdrachtgever bij het ontwikkelen en onderhouden van maatwerksoftware meer prioriteit geeft aan het ontwikkelen van de functionaliteit dan aan het op niveau houden van de onderhoudbaarheid van software, kan er technische schuld ontstaan. De opdrachtnemer neemt of krijgt niet genoeg tijd voor het op orde houden van de onderhoudbaarheid. Hierdoor kan op den duur zelfs een vicieuze cirkel ontstaan van meer technische schuld, dalende onderhoudbaarheid, meer nadruk op functionaliteit (want het kost zoveel tijd om de verandering te maken) en vervolgens nog meer technische schuld en een nog slechtere onderhoudbaarheid.

Voor dit risico biedt de NPR 5326 meerdere beheersmaatregelen. Een daarvan is het inzichtelijk maken van technische schuld en planmatige oplossing. Technische schuld wordt inzichtelijk gemaakt en planmatig aangepakt. De aanwezigheid van technische schuld heeft een nadelige invloed op de kwaliteit van de eindproducten. Het ontstaan van technische schuld gedurende een project is echter onvermijdelijk in de praktijk. Technische schuld kan zelfs een nuttig hulpmiddel zijn indien bewust toegepast: door bijvoorbeeld een stuk bestaande functionaliteit te kopiëren en aan te passen, is het soms mogelijk snel een nieuwe functie te realiseren. De technische schuld in de vorm van duplicatie tussen de originele en de gekopieerde broncode kan dan later worden opgelost. Het is daarnaast ook mogelijk dat een deel van de technische schuld bij aanvang van het project al bestond en mogelijk niet wordt opgelost.



In alle gevallen is het verstandig om te weten welke technische schuld er bestaat. Om te voorkomen dat technische schuld niet wordt opgelost en alleen maar toeneemt, is het zaak om het verminderen van technische schuld planmatig aan te pakken. Volg hiervoor de volgende stappen.

1. Meet de kwaliteit van de broncode en documentatie.
2. Maak inzichtelijk welke versies van derdepartijcomponenten en raamwerken worden gebruikt in de software en in hoeverre deze versies achterlopen.
3. Houd een issue log bij van technische-schuldissues.
4. Plan het oplossen van technische-schuldissues.
5. Los technische-schuldissues op.

Bedoeling NPR 5326

De NPR 5326 is primair bedoeld voor organisaties die maatwerksoftware laten ontwikkelen en voor organisaties die maatwerksoftware ontwikkelen voor zichzelf of voor andere organisaties. De NPR 5326 laat de relatie tussen opdrachtgever en opdrachtnemer zo veel mogelijk in het midden: de beheersmaatregelen zijn van toepassing als opdrachtgever en opdrachtnemer verschillende organisaties zijn, maar ook als beiden van dezelfde organisatie deel uitmaken. Een derde doelgroep zijn functionarissen die willen beoordelen in hoeverre opdrachtgevers en opdrachtnemers van maatwerksoftwareontwikkeling de risico's daarvan adequaat beheersen. Denk aan auditors of kwaliteits- en risicomangers.

Gebruik NPR 5326

De NPR 5326 kan op meerdere manieren gebruikt worden. Bij een aanbesteding van maatwerksoftwareontwikkeling zou een opdrachtgever potentiële opdrachtnemers kunnen uitnodigen aan te geven welke risico's voor de aanbesteding relevant zijn en hoe de opdrachtnemer denkt de risico's te zullen beheersen. Voor een opdrachtnemer kan het een middel zijn zich te onderscheiden van concurrenten door te laten zien voor welke risico's de opdrachtnemer al maatregelen heeft getroffen in haar standaard aanpak.

Geeft een opdrachtgever bij het ontwikkelen en onderhouden van maatwerksoftware meer prioriteit aan het ontwikkelen van de functionaliteit dan aan het op niveau houden van de onderhoudbaarheid van software, dan kan er technische schuld ontstaan

De NPR 5326 kan ook als input dienen voor het inrichten en verbeteren van een softwareontwikkelorganisatie. Bij de NPR 5326 zal een assessmentinstrument worden geleverd dat de risico's relateert aan de beheersmaatregelen. Veel beheersmaatregelen helpen meerdere risico's te mitigeren. Voor andere risico's zijn meerdere beheersmaatregelen nodig. Door in het assessmentinstrument de risico's die de organisatie of het project loopt te prioriteren, laat het instrument zien welke beheersmaatregelen het meest zullen bijdragen aan het beheersen van de geprioriteerde risico's.

De NPR 5326 kan verder gebruikt worden als referentiekader voor het beoordelen van een softwareontwikkelorganisatie. Door te onderzoeken welke beheersmaatregelen een organisatie al heeft geïmplementeerd en welke niet, of niet volledig, kan een risicoprofiel worden bepaald. Ook hier kan het assessmentinstrument hulp bieden: door de geïmplementeerde maatregelen in te vullen, laat het instrument zien welke risico's meer en welke minder goed beheerst worden. Uiteraard is dit geen exacte wetenschap: zowel de risico's als de beheersmaatregelen zijn in de NPR 5326 kwalitatief beschreven. Verwacht geen risicoscore tot op twee cijfers achter de komma.

AUDIT

MAGAZINE

Planning

Op het moment van schrijven is de werkgroep NPR 5326 bezig met het verwerken van het reviewcommentaar dat na de publieke consultatieronde begin januari 2019 is ontvangen. De planning is om voor de zomer een versie van de NPR 5326 aan de NEN op te leveren die inhoudelijk klaar is en dan redactioneel verwerkt wordt. En als alles goed gaat, volgt dan na de zomer de formele publicatie.

Noot

1. Armour, Phillip G., *Communications of the ACM*, vol. 43, nr. 10, oktober 2000.

Over

Frank Niessink is sinds 2017 kwaliteitsmanager bij ICTU. Daarvoor was hij adviseur op het vlak van softwarekwaliteit en procesverbetering en deed hij promotieonderzoek aan de Vrije Universiteit naar het verbeteren van softwareonderhoud.

Meer informatie over de kwaliteitsaanpak van ICTU vindt u op [ictu.nl/kwaliteitsaanpak](https://www.ictu.nl/kwaliteitsaanpak).

Tags: digitalisering, innovatie

Bron url: <https://auditmagazine.nl/artikelen/ontwikkelen-maatwerksoftware-riskante-onderneming/>