De prijs van imperfectie

Het is 23 september 1999. Na een reis van 286 dagen arriveert NASA's Mars Climate Orbiter bij onze buurplaneet. De bedoeling is om de sonde in een baan om Mars te brengen waar hij als weersatelliet zijn werk kan doen. Om 9:04:32 wordt het laatste signaal van de Orbiter ontvangen. Sindsdien is de satelliet spoorloos. Onderzoek van NASA wijst uit dat de Mars Climate Orbiter op Mars is neergestort. Oorzaak: een afrondingsfout in de besturingssoftware bij de conversie van engelse ponden naar kilo's.

Dit is maar één van de vele waargebeurde horrorverhalen over softwaredefecten die enorme schade hebben veroorzaakt. Er circuleren diverse lijstjes van dergelijke horrorverhalen op het Internet, zoals:
http://www5.in.tum.de/~huckle/bugse.html
http://infotech.fanshawec.on.ca/gsantor/Computing/FamousBugs.htm
http://www.cs.tau.ac.il/~nachumd/verify/horror.html

De vraag die elke softwareleverancier zich moet afvragen is: wat is de prijs van een defect in *mijn* software? De meeste softwarefabrikanten in Nederland bouwen bedrijfsmatige toepassingen waardoor mensenlevens niet direct in gevaar komen. Toch kunnen fouten veel schade veroorzaken bij zowel klant als leverancier. Reden voor softwarefabrikanten om goed te kijken naar de manier waarop ze software bouwen en defecten vermijden. Er is dan ook veel geschreven over softwarekwaliteit, denk onder andere aan Capability Maturity Mode (CMM).

In de praktijk blijkt een defect duurder te worden naarmate het later wordt gevonden. Een programmeerfout die direct door de programmeur zelf wordt gevonden kost ongeveer € 10 om te vinden en te verhelpen. Een vangnet voor defecten die niet door de programmeur worden ontdekt, is de softwaretester of testafdeling. Dergelijke fouten kosten ongeveer € 100 om te vinden en te verhelpen. Deze kosten zitten vooral in de loonkosten van zowel de tester als de programmeur. Veel tijd zit in de (mis-)communicatie tussen testers en programmeurs, problemen met reproductie, enzovoort. Als een defect pas door een klant wordt gevonden in de productieversie van de software zijn de kosten in beginsel niet meer te overzien. Zelf heb ik bij een vorige werkgever meegemaakt dat we programmeurs de halve wereld moesten rondsturen om problemen bij de klant te kunnen reproduceren en oplossen. De kosten van dergelijke defecten zitten niet alleen in loonkosten, vliegtickets en hotelovernachtingen, maar ook in zaken als een beschadigde reputatie.

Hoewel het continu verbeteren van ontwikkel- en testprocedures een belangrijke stap is om dergelijke fouten te voorkomen, blijven er defecten die moeilijk te vangen zijn. Vaak gaat het hierbij om softwarecode die conflicteert met andere, specifieke programma's zoals device-drivers. Of de fout treedt op in zeer specifieke situaties die onmogelijk allemaal van tevoren te testen zijn. Microsoft biedt nu een dienst aan die softwarefabrikanten helpt dergelijke problemen op te sporen en op te lossen. Deze dienst heet Windows Error Reporting en is te vinden op http://winqual.microsoft.com.

Het principe van Windows Error Reporting (WER) is dat als een programma crasht, de gebruiker wordt gevraagd hierover een error report te sturen naar Microsoft. Dit rapport is tussen de 50K en 100K groot en bevat onder meer een 'mini-dump' van het geheugen. Via WER kunt u als softwareleverancier snel inzicht krijgen in het aantal problemen dat gebruikers van de software op deze manier hebben aangemeld en de frequentie van de verschillende problemen, wat een indicatie is van de ernst van het probleem. Verder kunt u achterhalen of het probleem optreedt in combinatie met specifieke andere toepassingen (zoals device-drivers) en kunt u via de mini-dump in de debugger zien op welke regel het programma is gecrasht en wat er op dat moment op de stack stond. Met deze informatie is het in de meeste gevallen mogelijk om de oorzaak van het probleem te vinden en op te lossen.

Bovendien kunt u via WER instellen dat gebruikers die tegen een specifieke fout aanlopen vanaf nu een bepaalde boodschap te zien krijgen. Deze boodschap kan bijvoorbeeld een verwijzing bevatten naar een pagina op een website of een patch die de gebruiker kan downloaden om het probleem te verhelpen. Het is ook een goed idee om bij bètaversies van de software van WER gebruik te maken. Voor meer informatie over Windows Error Reporting, zie http://www.microsoft.com/netherlands/msdn/artikelen/wer.aspx

Het is onwaarschijnlijk dat NASA de crash van de Orbiter op Mars met WER had kunnen voorkomen, maar wellicht dat u wel de nodige crashes bij uw klanten kunt voorkomen, en daarmee de prijs van defecten in uw software aanzienlijk kunt verlagen.

Andreas de Ruiter
Developer & Platform Group
aruiter@microsoft.com