

In het nieuws

DIGITALE MELTDOWN

Is software te complex geworden?

We hebben computerprogramma's zo ingewikkeld gemaakt, dat we ze niet meer onder controle hebben en er een digitale meltdown dreigt, aldus berichten deze week. Wat zegt de wetenschap over de kans daarop?

Allereerst is de vraag wat met een digitale meltdown wordt bedoeld. 'Heb je het over tijdelijk niet kunnen handelen op de beurs, of dat we geen brood meer kunnen kopen?', slaat hoogleraar informatica Jan Friso Groote van de TU Eindhoven enkele piketpaaltjes. Een voorbeeld van de tweede categorie is een omvangrijke uitval van energiecentrales in de Verenigde Staten in 2003, waar een storing in een centrale een kettingreactie veroorzaakte die een groot deel van het stroomnet in het noordoosten van de VS platlegde. Dergelijke voorvallen zijn zeldzaam, maar kleinere incidenten gebeuren bijna dagelijks, zoals de problemen op de Nasdaq vorige week weer eens lieten zien.

Het is goed dat we veel taken toevertrouwen aan computers, zegt Groote. 'Een computer laat niet een trein te hard rijden omdat hij er even met zijn hoofd niet bij was vanwege een telefoontje.' Niettemin kan het ook goed mis gaan als taken uit handen worden gegeven aan de computer, zelfs met dodelijke afloop. Een bekend voorbeeld is het bestralingsapparaat Therac-25, dat als gevolg van softwarefouten soms onbedoeld dodelijke hoeveelheden straling afvuurde, waardoor in de jaren tachtig zeker vijf patiënten omkwamen.

Als er zaken misgaan, moeten we dat vaak achteraf constateren, zegt hoogleraar informatica Chris Verhoef van de VU. 'Terwijl dit eigenlijk vooraf moet gebeuren. Dat zie je bij de problemen op de Nasdaq, waar beurskoersen zomaar kelderen en de handel stilgelegd moet worden.' Een belangrijke sleutel is inputvalidatie: zorg ervoor dat de gegevens die gebruikers invoeren logisch zijn. 'Stel een handelaar wil 1 aandeel van 600 duizend yen verkopen, maar voert per ongeluk in dat hij

600 duizend aandelen van 1 yen kwijt wil. Het systeem zou dan moeten checken of er überhaupt zo veel aandelen zijn en het zou moeten waarschuwen dat de verkoopprijs wel erg laag is.' Met een simpele check is te voorkomen dat beurskoersen rare zwiepers gaan maken.

De fout kan ook verscholen liggen in de software. Moderne apparaten bevatten enorme hoeveelheden programmeer-

code. Als veel mensen gelijktijdig aan een systeem werken, weet niet iedereen wat iedereen doet, stelt Groote. 'Eigenlijk kan de mens de complexiteit van dergelijke systemen niet aan.' Gevolg: gemiddeld zitten er tien tot twintig programmeerfouten in elke duizend regels code. Een beetje software telt een miljoen tot honderd miljoen regels. Sommige van de bugs komen vrij snel naar voren, maar zeker bij nieuwe software die niet heel intensief getest is, zal een aantal onzichtbaar blijven. Vroeg of laat – in een combinatie van zeldzame omstandigheden – openbaren ze zich, soms met desastreuze gevolgen, zoals bij de Therac-25.

Soms kan software met de computer worden getest op bugs. Voor programmable logic controllers (plc), die worden toegepast in beveiligingssystemen, bestaan 'automatische stellingenbewijzers'. Daar gooi je een plc-programma in en stelt de vraag: kan deze brug ooit open als de slagbomen niet gesloten zijn? De automatische stellingenbewijzer loopt daarop alle mogelijke scenario's af en geeft dan – hopelijk – het antwoord nee. Probleem is dat bij grotere software het aantal variabelen sterk toeneemt, waardoor het aantal mogelijkheden zomaar kan oplopen tot 2 tot de macht 1000. Groote: 'Een getal groter dan er atomen in het heelal zijn.'

In de praktijk komt het erop neer dat softwaremakers het er maar bij laten zitten en als het misgaat van een menselijke fout spreken. Groote: 'Ze denken: we komen er wel mee weg. En vaak is dat zo.'

Bard van de Weijer

'Een computer laat niet een trein te hard rijden omdat hij er even met zijn hoofd niet bij was'