COLUMN CHRIS VERHOEF

Meer dan de som der onderdelen

Het behoeft nauwelijks uitleg, maar een auto, vliegtuig, of boorplatform is meer dan een enorme doos met onderdelen. Dat soort complexe artefacten moet voldoen aan een keur van eisen zoals emissierichtlijnen, veiligheid, stabiliteit, en meer. Daarnaast moet er ook sprake zijn van integrale systeemprestaties. Denk aan remmen, opstijgen, landen, olie oppompen, enzovoort. Uiteraard heb je wel alle onderdelen nodig om daarmee die integrale systeemprestaties te leveren. Sterker, die onderdelen op zich moeten allemaal aan bepaalde kwaliteitseisen voldoen. Metaalmoeheid in de autovering, en het ding zakt met 120 kilometer per uur door zijn hoeven. Hoogtemeter niet op orde, en de automatische piloot zet de landing te vroeg in. Hitteschildje beschadigd, en de spaceshuttle verbrandt in de dampkring. De gevolgen zijn bekend.
We zien dus dat bij complexe systems-engineeringprojecten de integrale systeemprestatie door een enkel onderdeel danig in de war gebracht kan worden. Niet alleen weigerachtige onderdelen, maar ook de integratie van allemaal op zich goed werkende onderdelen kan voor grote problemen zorgen. Een prima werkende benzine-injectie en een prima werkende uitlaat kunnen toch zorgen voor een auto die niet aan de emissierichtlijn voldoet.

Omgeving waarin software moet werken, wordt maar al te vaak uit het oog verloren

Ook in de IT zien we dit fenomeen. Een verzameling van prima werkende onderdelen kan toch tezamen zorgen voor een niet werkend veiligheidssysteem bij de hogesnelheidslijn; het European Rail Traffic Management System (ERTMS). Of – zo konden we onlangs in de krant lezen: 'Het testen van de veiligheids-systemen in de Roertunnel en Swalmentunnel van de A73-Zuid tijdens de sluiting afgelopen weekend, is redelijk verlopen. Alle 52 veiligheidssystemen functioneren afzonderlijk naar behoren, maar als ze bij een calamiteit samen in werking moeten treden, gaat het mis.' Kennelijk praten we hier net als bij de HSL niet over een laatste tunneltechnische trivialiteit: 'Het is nog steeds onduidelijk wanneer de laatste testfase van het veiligheidsysteem plaatsvindt.' Aldus Rijkswaterstaat.
Je hebt dus niets aan goed werkende onderdelen of componenten als de integrale systeemprestatie niet geleverd kan worden. Maar zelfs als je met goed werkende onderdelen, en een goed geslaagde integratie, een heuse systeemprestatie weet neer te zetten – dan nog ben je er niet. Het gehele systeem moet ook nog goed in zijn omgeving gedijen. Een bekend voorbeeld is dat het systeem geen andere systemen stoort, en dat het systeem niet door andere systemen kan worden gestoord. In jargon is dat de EMI/EMC-vraag (EMI/EMC = electromagnetische interferentie en compatibiliteit). Alledaagse interferentie maken we mee als we via de radio of computer al horen dat de mobiel dra af zal gaan. De mobiel levert weliswaar een systeemprestatie maar stoort andere systemen wel degelijk. Daarom zien we bij intensivecare-units van ziekenhuizen bordjes met mobieltje uit. En dito bij vliegtuigen. Omgekeerd, als we langs radiozendmasten rijden, zoals vlak bij de VU op de A10, dan is de radio-ontvangst bij sommige autoradio's minder tot afwezig. Dat is een EMC-probleem: die FM-ontvangers laten zich storen door andere systemen.
Lastiger wordt het als de cruisecontrol op hol slaat of de ABS weigert door EMI/EMC-problemen. Onvoldoende EMC-hardheid laten de bits en bytes van een boardcomputer doen geloven dat er met constante snelheid gereden moet worden of dat een ABS-remming onnodig is. Of, wat ik zelf eens meemaakte: mijn auto wilde niet meer open, door een EMI/EMC-probleem. Door interferentie van de omgeving en onvoldoende EMC-hardheid van de systemen in de auto was de enige mogelijkheid om het ding 50 meter verderop te duwen waarna het probleem weg was. De lokale bevolking wist me te melden dat ik mijn auto op een bekende hotspot had geparkeerd.

Wat ik maar al te vaak meemaak in de praktijk is dat systeemontwikkeling te snel in te veel details verzand. De integraliteit wordt daarmee volkomen uit het oog verloren, laat staan de omgeving waarin het systeem wordt geacht te werken. Op onderdelen kan deelfunctionaliteit geïsoleerd prima werken, maar als het op integratie aankomt, is de visie zoek. En het systeemgedrag ook. Een ander daarbij behorend verschijnsel is dat er vaak niemand verantwoordelijk is voor de integrale systeempresentatie of belangrijke onderdelen daarvan. Bijvoorbeeld naast een hoofdarchi-tect (bouwmeester) bij een ERTMS of A73 zou ook een integrale safety engineer niet misstaan.

Prof. dr. Chris Verhoef is hoogleraar Informatica aan de Vrije Universiteit Amsterdam

Internetprotocoll en zijn gevaar

Overheid moet regisserende rol vervullen op het geb ied van internetbeveiliging

Internetprotocollen zijn kwetsbaar en kunnen veel schade toebrengen aan de Nederlandse samenleving. Het huidige overheidsbeleid is niet toereikend, zeggen **Bart Knubben** en **Dennis Baaten**. De overheid moet de marktpartijen stimuleren samen de problemen aan te pakken.

ILLUSTRATIE: JOS THOMMASSEN

De Nederlandse overheid ziet 'toegang tot internet' als een vitaal element voor de Nederlandse samenleving. Verstoring of uitval van een vitaal element kan volgens de overheid grote economische of maatschappelijke ontwrichting op (inter)nationale schaal veroorzaken en direct of indirect tot veel slachtoffers leiden. Kortom, de overheid vindt de veiligheid van internet erg belangrijk. Recente kwetsbaarheden in internetprotocollen tonen echter aan dat het huidige overheidsbeleid niet toereikend is.
Onverstoorde toegang tot internet kan met de huidige overheidsmaatregelen onvoldoende worden gegarandeerd. Kwetsbaarheden in internetprotocollen maken het mogelijk om op grote schaal websites plat te leggen of gevoelige informatie te stelen, terwijl oplossingen vaak niet door één partij kunnen worden gerealiseerd.
Recentelijk zijn er verschillende ernstige beveiligingsproblemen opgedoken met betrekking tot internetprotocollen. Vooral het door Dan Kaminsky ontdekte DNS-lek (midden 2008) zorgt voor de nodige commotie, maar ook in protocollen zoals BGP en SSL zijn kwetsbaarheden opgedoken. Deze protocollen standaardiseren de wijze waarop informatiesystemen met elkaar over internet communiceren en zijn geïmplementeerd in applicaties of besturingssystemen.
Juist op het niveau van internetprotocollen kunnen zich grote risico's voordoen omdat deze het fundament vormen van het internet. Het zijn gemeenschappelijke functies van internet die door iedereen worden gebruikt. Deze gemeenschappelijkheid is enerzijds de kracht van een protocol en zorgt voor interoperabiliteit. Anderzijds vormt de gemeenschappelijkheid een zwakte omdat een kwetsbaarheid iedereen raakt en vaak niet door één partij kan worden opgelost.

Veel internetprotocollen beginnen op leeftijd te raken en zijn vaak niet of nauwelijks ontworpen vanuit een beveiligingsperspectief. De verwachting van verschillende experts is dat in de toekomst nog meer ernstige kwetsbaarheden zullen opduiken. Zo schrijft Dan Kaminsky op zijn blog dat veel kwetsbaarheden in internetprotocollen de kern van het internet raken en nu en in de toekomst een bedreiging vormen voor onze wereldwijde infrastructuur. Kaminsky benadrukt het belang om te komen tot oplossingen voor deze kwetsbaarheden. Kwetsbaarheden in internetprotocollen kunnen verschillende oorzaken hebben. De oorzaak kan gelegen zijn in de specificatie van een protocol of, wanneer de specificatie geen beveiligingsfouten bevat, in de implementatie van een protocol. We gaan ervan uit dat een kwetsbaarheid in de specificatie ook een kwetsbaarheid in de implementatie tot gevolg heeft.
Het risico van een kwetsbaarheid is afhankelijk van aspecten zoals het aantal getroffen gebruikers, de aangeboden diensten die afhankelijk zijn van het kwetsbare protocol (bijvoorbeeld internetbankieren in geval van SSL), de criminele businesscase, het ICT-updatebeleid bij organisaties, en de toegankelijkheid tot de benodigde kennis om de kwetsbaarheid te misbruiken. Bij een kwetsbaarheid in de specificatie van een internetprotocol is het risico vaak erg groot omdat zeer veel tot alle gebruikers worden getroffen en aan internet gekoppelde systemen in principe vanuit de hele wereld benaderbaar zijn.

DNS-lek kan niet worden opgelost door één enkele partij

Neem het hierboven genoemde DNS-lek, waardoor hackers internetverkeer kunnen omleiden naar hun eigen servers en daardoor bijvoorbeeld wachtwoorden, e-mails en bankgegevens kunnen onderscheppen. In Amerika liep vorig jaar 10 procent van de bedrijven tegen DNS-gerelateerde incidenten aan, ten opzichte van 2 procent in 2007. Deze stijging wordt in verband gebracht met het genoemde DNS-lek. Dit voorbeeld laat zien dat de impact van een kwetsbaarheid in een internetprotocol zeer omvangrijk kan zijn, en geeft aan dat het belangrijk is om dit soort kwetsbaarheden tijdig en effectief aan te pakken door het nemen van gepaste maatregelen.
Een maatregel bestaat uit een technisch en organisatorisch deel. Bij kwetsbaarheden in internetprotocollen is met name het organisatorische gedeelte een uitdaging. Dit komt mede door het gemeenschappelijke karakter van een internetprotocol en doordat het eigenaarschap van internet niet eenduidig is belegd. Technisch gezien zijn er vaak degelijke maatregelen voorhanden, maar de uitdaging zit hem in de organisatie van het doorvoeren van de maatregel. Afhankelijk van de oorzaak en risico's van een kwetsbaarheid, stijgt de noodzaak tot afstemming en samenwerking tussen verschillende belanghebbenden zoals: internetaanbieders (ISP's), softwareleveranciers en gebruikers(groepen); zie kader en tabel.
Op dit moment zijn er verschillende Nederlandse overheidspartijen actief rondom internetbeveiliging. GOVCERT.NL informeert en adviseert de Nederlandse samenleving over kwetsbaarheden en oplossingen. Digibewust.nl probeert het bewustzijn van burgers en bedrijven omtrent beveiligingsrisico's te vergroten. Het KLPD en de AIVD spelen met name op het vlak van opsporing en inlichtingen een rol. Het overheidsinitiatief NICC brengt diverse publieke en private partijen bij elkaar ter bestrijding van cybercrime.

Voor het bestrijden van kwetsbaarheden waarvoor leveranciers onafhankelijk van elkaar een oplossing kunnen aanbieden (zie tabel: niveau 1) lijkt de huidige aanpak van de overheid goed te werken. Mede door de onafhankelijke informatieverstrekking van de overheid vindt marktwerking plaats. Internetserviceproviders (ISP's) kunnen zich bijvoorbeeld onderscheiden van hun concurrenten door middel van hun softwarekeuze en updatebeleid. Dit onderscheidend vermogen is er vaak niet wanneer een kwetsbaarheid wordt veroorzaakt door een risico in de protocolspecificatie (zie tabel: niveau 3). Het gemeenschappelijke karakter van een internetprotocol conflicteert met de mogelijkheid tot het creëren van onderscheidend vermogen. Daarom is de huidige rol van de overheid bij het aanpakken van kwetsbaarheden omtrent internetprotocollen onvoldoende.
Illustratief voor de huidige situatie is dat maatregelen tegen het DNS-lek voor het '.nl'-domein nog steeds onduidelijk zijn. Hoewel GOVCERT.NL een vrijblijvend advies op zijn website heeft gepubliceerd, lijkt de markt een afwachtende houding aan te nemen. Uiteraard zijn er lokale noodverbanden en pleisters aangebracht, maar de plannen voor een fundamentele oplossing zijn onduidelijk. Een woordvoerder van Stichting Internet Domeinnaamregistratie (SIDN), aan wie de overheid het beheer van het '.nl'-domein heeft toevertrouwd, geeft aan dat SIDN de implementatie van DNSSEC, dat als oplossing wordt gezien voor het ontdekte DNS-lek, dit jaar oppakt. Er zijn echter geen concrete plannen bekend gemaakt. Het is onduidelijk of en, zo ja, hoe bedrijven en overheden aanhaken bij de implementatie van DNSSEC. Dit laatste is van groot belang, omdat het DNS-lek niet structureel opgelost kan worden door één enkele partij. DNSSEC heeft alleen effect wanneer dit voor het gehele '.nl'-domein wordt geïmplementeerd; het negatieve netwerkeffect. Dit benadrukt de noodzaak tot samenwerken van verschillende partijen zoals SIDN, ISP's en bijvoorbeeld banken.
Gezien de ernst van de situatie heeft de Amerikaanse overheid recentelijk besloten om maatregelen te treffen: het '.gov'-domein (voor Amerikaanse overheidswebsites) wordt overgezet naar het veiligere DNSSEC. Landen als Brazilië (.br), Bulgarije (.bg), Tsjechië (.cz), Puerto Rico (.pr) en Zweden (.se) zijn reeds overgestapt op DNSSEC. Het Verenigd Koninkrijk, Duitsland en Rusland zouden ook werken aan een overstap. Bij veel van deze buitenlandse initiatieven vervult de overheid wel een stimulerende en coördinerende rol.

De Nederlandse overheid dient een regisserende rol te vervullen met betrekking tot beveiligingsrisico's die zich manifesteren in de gemeenschappelijke functies van het internet. Kwetsbaarheden in internetprotocollen treffen namelijk grote aantallen burgers, bedrijven en overheden, én kunnen vaak niet door één marktpartij worden opgelost. Dit soort kwetsbaarheden kunnen de vitaliteit van het internet ernstig bedreigen.

Overheid moet regisseren, geen marktactiviteiten overnemen

De regisserende rol dient duidelijk belegd te zijn bij één (bestaande of nieuwe) organisatie. Deze rol houdt niet in dat de overheid marktactiviteiten moet overnemen. Vanuit haar regisserende rol mobiliseert en stimuleert de overheid juist marktpartijen, zodat problemen in gezamenlijkheid worden opgepakt. Daarnaast zorgt de regisseur ervoor dat de maatschappij geïnformeerd wordt over de aanpak van fundamentele kwetsbaarheden. Waar nodig is er afstemming op internationaal niveau. Op deze manier ontstaat er gezamenlijke aandacht om tijdig te komen tot concrete oplossingen en eenduidige communicatie, zodat de kans op grootschalige verstoringen en uitval van het internet wordt geminimaliseerd. Kortom: internetsecurity vergt gepaste overheidsregie.

Mr. drs. Bart Knubben en ir. Dennis Baaten (dennis.baaten@vka.nl) zijn als adviseurs werkzaam bij Verdonck, Klooster & Associates (http://www.vka.nl). Beiden hebben ruime ervaring op het gebied van internetsecurity. VKA is een onafhankelijk adviesbureau op het snijvlak van strategie, procesinrichting en ICT.

Voor reacties en nieuwe bijdragen van deskundigen: Henk Ester (h.ester@sdu.nl, (070) 378 03 97).

Organisatorische complexiteit

Niveau	Specificatie	Implementatie	Betrokken leveranciers	Maatregel	Complexiteit
1	Veilig	Niet conform specificatie; onveilig	Eén of meerdere	Software-update(s)	Beperkt tot aanzienlijk
2	Onveilig, maar herstelbaar	Conform specificatie	Alle	Specificatie-update, gevolgd door softwareupdate(s)	Aanzienlijk tot hoog
3	Onveilig, niet herstelbaar	Conform specificatie	Alle	Migratie naar nieuw protocol	Hoog tot zeer hoog

Wanneer softwareleveranciers een beveiligingsfout in de implementatie van een internetprotocol maken, wordt dit opgelost door middel van leverancierspecifieke software-updates die gebruikers kunnen installeren (niveau 1). Het kan ook zo zijn dat het protocol conform specificatie is geïmplementeerd, maar dat de specificatie een beveiligingsrisico bevat. In sommige gevallen is deze specificatiefout herstelbaar (niveau 2). De specificatie van het protocol dient te worden geüpdatet, waarna alle leveranciers een software-update conform de nieuwe specificatie kunnen uitbrengen.
De organisatorische complexiteit van de maatregel is het grootst als er een beveiligingsrisico in de specificatie voorkomt dat niet herstelbaar is (niveau 3). Bijvoorbeeld omdat het protocol verouderd of achterhaald is. Er dient dan uitgeweken te worden naar een ander of nieuw protocol. In zo'n geval is er vaak sprake van een negatief netwerkeffect, omdat de maatregel pas volledig effectief is wanneer iedereen migreert naar het nieuwe protocol; een ketting is zo sterk als zijn zwakste schakel.