DE KEUS VAN INGENIEUR TEUS

ir. Teus van der Plaat

IT`S GREAT, IT`S FANTASTIC, WE BUILD A WALL!

Dit zijn bekende kreten van een bevriend staatshoofd. Hebben deze kreten ook inhoud? Ik heb meerdere redenen om deze kreten ook te hanteren bij een aantal recente persoonlijke en innovatieve IT ontwikkelingen, die in mijn ogen zeker inhoud hebben.

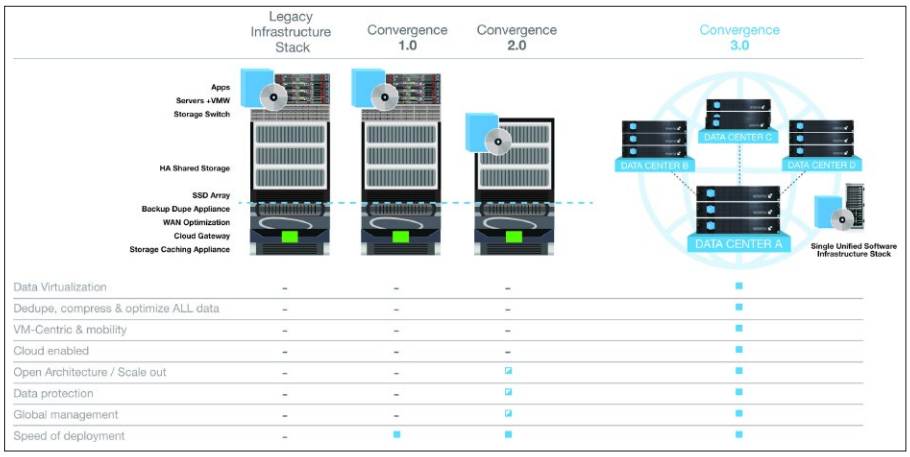
It's great, it's fantastic 1

Via dit medium wil ik mijn dank uitspreken voor het feit dat ik samen met een aantal anderen verkozen ben voor de prestigieuze Intercom award. Elders in dit nummer zult u er ongetwijfeld over lezen. Het is voor mij een stimulans om door te gaan met het schrijven van columns over actuele ICT zaken. Het is voor mij een hobby om bij te blijven in de snel veranderende wereld van de ICT. Vroeger was je bevoorrecht omdat je als medewerker van Defensie altijd door de industrie als eerste op de hoogte gebracht werd van de nieuwste ontwikkelingen. Defensie was vaak de eerste die zaken tot ontwikkeling bracht, zoals bijvoorbeeld de GPS en spread spectrum radio systemen. Sinds een aantal jaren is dat echter volledig omgedraaid. In de 'buitenwereld', die gedomineerd wordt door de consumentenmarkt gaat alles razendsnel en tegenwoordig is bijna alles gewoon openbaar op internet te volgen. Als je weet hoe en waar je moet zoeken kun je bijna alles vinden op internet.

It's great, it's fantastic 2 – the best

Een ontwikkeling, die al enkele jaren aan de gang is, en waar ik het nog niet over heb gehad is de opkomst en snelle ontwikkeling van de zogenaamde *hyperconverged* systemen. Deze systemen kenmerken zich door de samenvoeging van een aantal componenten, die vroeger en bij veel bedrijven nog steeds separaat bekeken werden en worden. Het gaat hierbij om de server, het netwerk en de storage, die in een fysieke hardware unit worden ondergebracht. Daarnaast zijn er ook diverse software onderdelen die op deze omgeving worden aangeboden.
Men spreekt vaak over gecertificeerde systemen waarbij de leverancier van de *hyperconverged* omgeving alle standaard hard- en softwarecomponenten nauwkeurig op elkaar heeft afgestemd. Want ondanks het feit dat er gebruik gemaakt wordt van standaard processor, storage eenheden als SSD's en spindels is er voor de software een afhankelijkheid van de onderliggende hardwareconfiguratie. Zeker als er ook gebruik gemaakt wordt van virtuele systemen zoals VMware met daarop draaiend systemen als SAP is het zaak garanties te krijgen op de goede werking van het geheel.

Er zijn leveranciers die zeer geavanceerde complete systemen leveren, zoals NETAPP, DELL en HP, maar er zijn ook leveranciers van software, die op standaard componenten van verschillende leveranciers kunnen draaien. Voorbeelden hiervan zijn NUTANIX en Simplivity, welk laatste bedrijf recent voor 650 miljoen dollar is overgenomen door HP.
Het zijn zogenaamde *scale out* systemen. Als er een capaciteitstekort is kunnen gelijksoortige systemen min of meer onbeperkt worden bijgeschakeld waarbij dan alle omgevingen tegelijkertijd worden uitgebreid. (Compute, Storage, Network). De onderlinge verbindingen tussen de systemen zijn gebaseerd op snelle glasvezelverbindingen, die zich over relatief grote afstanden kunnen uitstrekken. De limiterende factor hierbij is de latency van deze verbindingen. Het licht gaat immers niet sneller dan 300.000 km per seconde en



een vertraging van meer dan enkele milliseconden is voor sommige toepassingen al te veel.

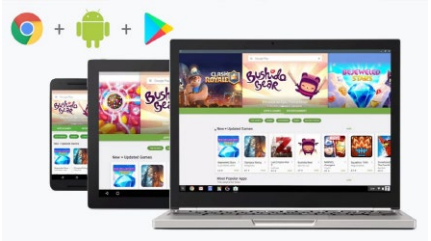
Diverse leveranciers bieden tegenwoordig ook asynchrone systemen die goed om kunnen gaan met enige latency waardoor de systemen over grotere afstanden van elkaar verwijderd kunnen zijn. Hiermee kunnen gedistribueerde systemen met 32 tot 64 nodes gemaakt worden die voor de applicaties als een platform gelden. Hierbij is dan de back-up *recovery* volledig gegarandeerd want een kenmerk van deze systemen is dat uitval van een of meer componenten geen invloed heeft op de beschikbaarheid van de applicaties.

Voor militair gebruik waarin overleefbaarheid bij uitval van systemen een must is zijn dergelijke systemen als *Its Great, Its Fantastic* te kwalificeren, omdat er diverse nodes kunnen uitvallen zonder dat de applicaties uitvallen.
Deze kunnen volledig dynamisch geswitched worden, inclusief hun data. Er openen zich hiermee hele nieuwe mogelijkheden om grote geografische spreiding te realiseren waardoor de beschikbaarheid onder alle omstandigheden zeer hoog kan blijven.

It's great, it's fantastic 3

In een vorige column heb ik geschreven over de beschikbaarheid van de 2 miljoen Android applicaties op de Chromebook computers. Begin januari op de CES in Las Vegas en ook in de maanden erna is er een heel scala van nieuwe Chromebook computers aangekondigd. In feite zijn het tablets met een toetsenbord. Het toetsenbord kan 360 graden gedraaid worden achter het display. Ook een aantal van deze nieuwe systemen is Milspec vanwege hun toepassing in schoolomgevingen.

Hoewel de Android apps nog niet allemaal vlekkeloos draaien is er onmiskenbaar een nieuw tijdperk ingetreden. In volgende Chrome OS versies, die met grote regelmaat verschijnen, zullen de Android apps zich automatisch aanpassen aan de schermgrootte.



Het Chrome OS staat bekend om zijn immuniteit voor virussen. Google heeft na een aantal jaren, medio vorig jaar het bedrag dat uitgekeerd wordt na een te reproduceren hack op een Chromebook verhoogd van 50.000 naar 100.000 dollar en... het is nog steeds stil.
Volgens Google zijn er nog geen bedragen uitgekeerd. De authenticatie op de Chromebooks is nu ook mogelijk via vingerafdruk scanners en via authenticatie op de smartphone. Hierdoor wordt two factor authenticatie min of meer standaard mogelijk, hetgeen de security enorm verhoogd. Volgens de laatste berichten is het marktaandeel op scholen wederom groter geworden.

It's great, it's fantastic 4 – We build a wall

De firma Cyberinc is recent in Europa op de markt gekomen met een hele bijzondere firewall. Hij bestaat uit een appliance die buiten de gewone firewall wordt geplaatst (in een DMZ) waarin in virtuele machines browsers draaien. De gebruiker achter zijn PC of in de toekomst ook op zijn smartphone heeft een speciale HTML5 applicatie waarmee encrypted verbinding gezocht wordt met de appliance. In de appliance vindt een kopieerslag plaats op video-pixel-niveau van het beeld van de browser die daadwerkelijk het internet op gaat.

De browser die draait op de werkplek gaat alleen naar de appliance. In feite is dit hetzelfde principe zoals bij defensie al jaren IODW werkt. Het verschil is echter dat de performance veel beter is en dat alle soorten platformen en browsers worden ondersteund. Ook video en Skype worden op deze wijze op het intranet mogelijk. Er is een hele beheer omgeving rond de appliance waarmee alles gemonitord en bestuurd kan worden. Per appliance zijn afhankelijk van het model duizenden simultane sessies mogelijk. Deze appliance is dus ook net zoals IODW bestand tegen de zogenaamde *Zero Day Exploits*, er is immers een onderbreking van de IP-stroom en er vindt een kopieerslag plaats.

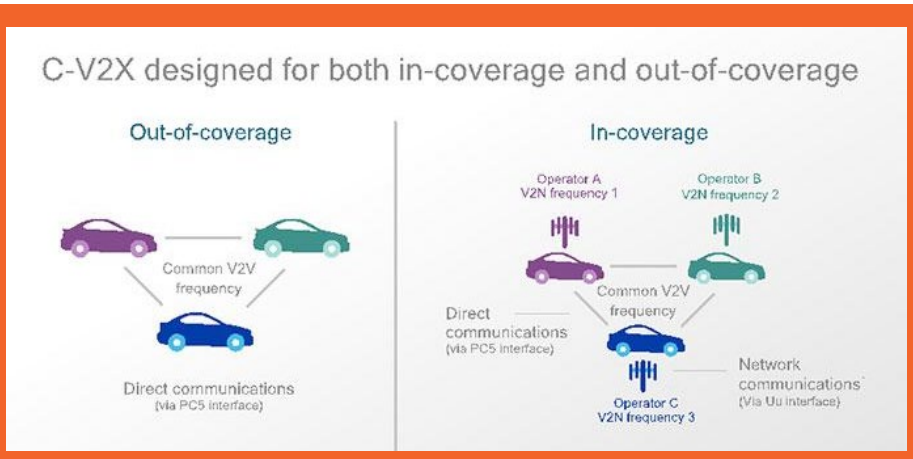
It's great, it's fantastic 5

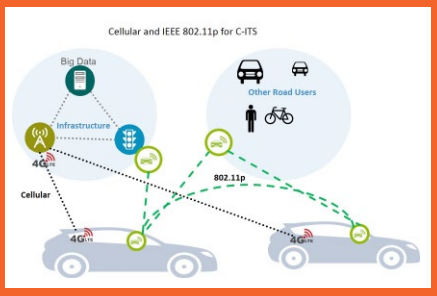
Op het gebied van de zelfrijdende auto zijn er ook weer significante vorderingen gemaakt. Zo meldde Google dat het aantal menselijke interventies per 1000 mijl in december 2016 gedaald was naar 0.2. Dat wil zeggen eenmaal in de 5000 mijl is er een ingreep door de chauffeur.

Dat wil overigens nog niet zeggen dat deze ingreep een ongeluk heeft voorkomen, want naar schatting is dat in slechts 20% van de ingrepen het geval. Ook als er een onvolkomenheid in het zelf rijden is volgens de bestuurder wordt er ingegrepen. Een jaar geleden was dat nog een ingreep per 1000 mijl.

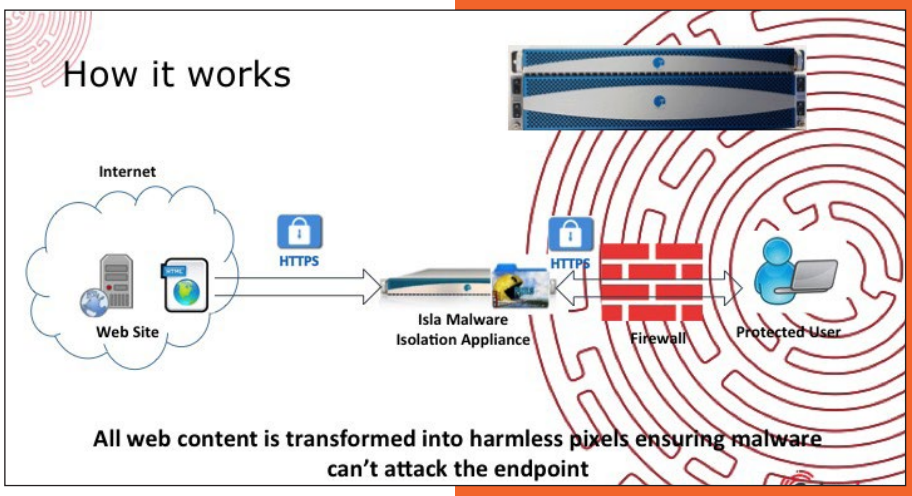
De staat Californië publiceert alle data van alle testauto's die er daar rondrijden. BMW zat nog op 1,5 ingreep per 1000 mijl in Californië. Naar verluid zouden Tesla en Uber daar niet meer meedoen omdat men niet wil dat hun cijfers publiek worden. De auto van Uber was namelijk door een rood stoplicht gereden in San Francisco. Aannemelijk is dat het steeds moeilijker wordt om het aantal ingrepen verder omlaag te dringen, want het spreekwoord de laatste loodjes wegen het zwaarst zal hier ook wel gelden. Duidelijk is dat Google hier mijlen ver voorligt op de competitie.

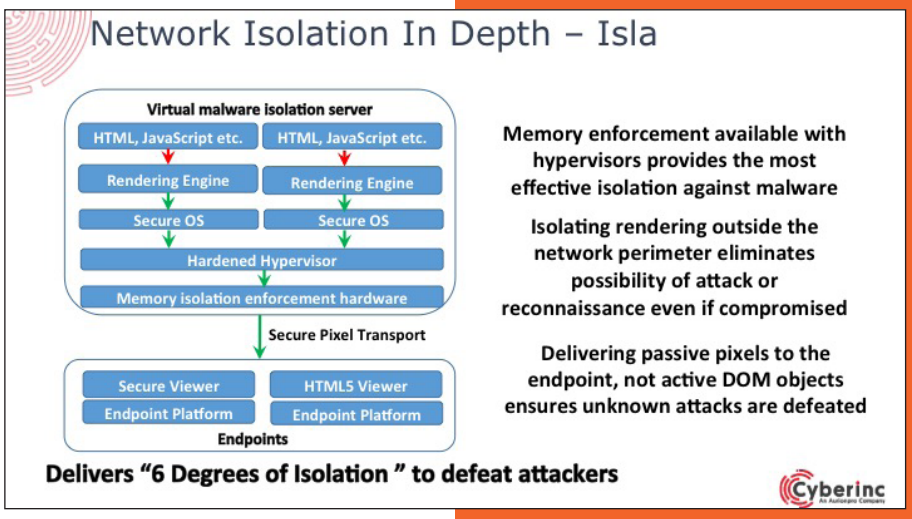
Op het gebied van de V2X standaarden worden grote vorderingen geboekt, immers in de zomer 2017 valt het doek en worden ze bevroren voor implementatie in de 3GPP release 14. Het gaat hierbij dus om standaardisatie van de *Vehicle to Vehicle*, de *Vehicle to Pedestrian*, de *Vehicle to Infrastructure* en de *Vehicle to Network* standaarden, die verlopen via de 4G-netwerken van de mobiele operators. Er is wel een hele discussie aan de gang tussen de voorstanders van het 802.11P protocol dat in de USA voorgeschreven wordt voor autonoom rijdende auto's, die zonder tussenkomst van mobiele netwerken met elkaar praten via de 5,9 GHz-band met een beperkte reikwijdte en de voorstanders van de V2X protocollen.





De Firma Qualcomm die van plan is de chipsets te gaan verkopen heeft inmiddels chipsets beschikbaar die beide protocollen ondersteunen.
Als er geen netwerkdekking is kan een auto hierbij altijd op het 802.11P protocol terugvallen, maar zodra er weer een 4G-netwerk is kunnen auto's met hele lage latency over veel grotere afstanden met elkaar communiceren.
Beide protocollen zullen zeker ook in de toekomstige militaire setting van grote invloed zijn op nieuwe vormen van communicatie tussen militaire entiteiten van staal en vlees en bloed. Te hopen is dat er voldoende aan de beveiliging van dergelijke protocollen is gedacht, want ook hier ligt de cyberdreiging vanaf het eerste moment op de loer.





Er is dus van alles aan de hand op het gebied van IT-innovatie. Met recht kunnen we dus de kreet It's great, it's fantastic gebruiken om aan te geven dat deze innovatieve ontwikkelingen werkelijk van belang zijn. Er wordt met het Cyberinc product zelfs daadwerkelijk een zero day capable wall gebouwd, waar in dit geval de Mexicanen niet voor hoeven te betalen, maar wel de ondernemingen die het ding aanschaffen om zichzelf te beschermen.