TER LAND TER ZEE, IN DE LUCHT, MAAR VIA IP IS DE DATA OP DE VLUCHT

Ir. M.R. Oberman (inzet foto) en ing. V.M. Kroon,
Oberman Telecom Management Consultants BV

Het gaat in dit artikel niet om de lezersgroep van Intercom als datagebruikers, het gaat om de integrale data, die via een communicatie-infrastructuur bereikbaar is, van Nederland BV en daardoor als gevolgeffect de continuïteit van Nederland BV en dus ook, juist de bewaking en borging daarvan. Dit artikel bestaat uit vier delen. Het eerste deel is een beknopt historisch perspectief dat leidt van papieren communicatie tot en met de elektronische communicatie. Het tweede deel gaat dieper in op de onomkeerbare weg die digitale communicatie en met name op IP gebaseerde communicatie in de maatschappij aan het innemen is. Het derde deel gaat in op de toepassingen en de gevolgen van de toepassingen voor de maatschappij. Afgesloten gaat worden met de implicaties van het voorgaande, in feite: 'what is next, to exist in our digital world', vanuit OTMC als onafhankelijk adviesbureau.

OVER DE AUTEURS

Maarten Oberman en Vincent Kroon zijn beiden werkzaam bij Oberman Telecom Management Consultants bv, onafhankelijk adviesbureau voor data- en telecommunicatie. Dit adviesbureau is al meer dan 20 jaar toonaangevend in het werkveld. Voor Defensie heeft zij onder andere, in nauw overleg, de vernieuwing van de telefonie-transitlaag (MDTX) georganiseerd in 2004-2006.

HET HISTORISCH PERSPECTIEF

Communicatie, in al zijn verscheidenheid, is de basis en de stimulans voor de ontwikkeling van veel processen in organisaties en bedrijven. De ontwikkeling van communicatiemiddelen is weliswaar al eeuwen oud, maar was tot voor 1950 primair gericht op middelen voor afstandsoverbrugging en nauwelijks gericht op faciliteiten om te communiceren met verschillende informatiesoorten, tijd, plaats en vorm onafhankelijk. De ontwikkeling van communicatiefaciliteiten en toepassingen in de breedte en in samenhang tussen verschillende informatiesoorten heeft pas na 1980 plaatsgevonden, met het accent van deze ontwikkelingen op de laatste vijftien jaar.

Inmiddels is er een veelheid aan andersoortige communicatiefuncties ontstaan, zoals videocommunicatie, e-mail, tekstmessaging, integratie van voicemail met e-mail, adresboek gekoppeld aan telefoonnummers, e-mailadressen en agenda en de verschuiving van deze functies naar toepassingsgerichte e-mail, de social media communicatie. Anno 2012 worden er meer databits dan spraakbits verzonden in de netwerken van diverse operators. Door de verschuiving in type bittransport, andere informatiesoorten dan spraak dus, wordt ook duidelijk dat die andere communicatietoepassingen snel relevanter aan het worden zijn dan spraak in het totale palet aan communicatiefaciliteiten. Deze verschuiving wordt nog versterkt, doordat het inmiddels mogelijk is om beeldinformatie, plaatsbepalingsinformatie, apparaatpositiegegevens, directe gebruikers en vrijwel alle soorten gebruikersomgevingsinformatie, scan- en andere sensorinformatie te combineren en te laten interacteren met elkaar, in tot voor kort nog ongekende mogelijkheden.

De toename van deze faciliteiten is gekomen toen ICT-middelen ook de basis werden van de communicatiemiddelen en daarmee van de communicatietoepassingen.
Tegenwoordig is dus de communicatie gericht op de uitwisseling van informatie en de conversie van data uit sensoren naar informatie en de interactie tussen de verschillende informatiesoorten via communicatiefaciliteiten en –toepassingen. Daardoor zijn communicatietoepassingen een integraal onderdeel van alle bedrijfs- en organisatieprocessen geworden. Inmiddels is het dan ook zo ver dat zonder de werking van de communicatie-infrastructuur een bedrijf of organisatie niet meer functioneert en geleidelijk degenereert en tenslotte expireert. Daardoor is ook keuze en de ontwikkeling van de communicatietoepassingen en de betrouwbaarheid in combinatie met continuïteit cruciaal geworden voor de bedrijfsperformance van alle individuele bedrijven en organisatie, maar ook collectief, Nederland BV

Communicatietoepassingen zijn eigenlijk het primaire bedrijfsproces

Gas, water, licht en IP?
Gas, water en licht vormden al vele eeuwen de basis voor het functioneren van organisaties en de maatschappij. Elektronische communicatie op basis van het communicatieprotocol IP is daar de afgelopen jaren ook onderdeel van geworden, omdat elk communicatieapparaat zonder IP-connectie niet meer werkt, of het nu gaat om besloten bedrijfsnetwerken of dat het gaat om openbare netwerken of het openbare internet. IP is dus ook uw basisinfrastructuurvoorziening geworden, inmiddels uw onmisbare voorziening. Uitval van IP betekent namelijk geen communicatiefaciliteiten meer. Het effect van geen IP is ongemak, schade, ontbreken van informatie, stilstand, maar ook geen financiële transacties meer. In het verlengde is een langere afwezigheid van IP-connectie de opmaat naar achterstand, wanorde, chaos en onherstelbare schade en uiteindelijk bedrijfseconomische gevolgen voor elke organisatie en dus de maatschappij.

IP is de basis van elke communicatietoepassing

Voor die enkele communicatiesystemen die IP nu overigens nog niet als basisdrager hebben, komt het moment vanzelf dat ook daar IP de basisdrager van gaat worden. In de telefoniesystemen heeft de IP-revolutie zich afgespeeld ten koste van de traditionele telefooncentrale ofwel de PABX. De overgang van de PABX naar een VoIP-infrastructuur gaat nog steeds razendsnel.
Deze overgang naar IP geldt echter ook voor andere informatie- en communicatietoepassingen zoals videocommunicatie en videostreaming en tekstberichten in de bedrijfsomgeving en de informatie- en communicatiefaciliteiten in het openbare internet. Hierdoor is er synergie ontstaan tussen de functionaliteiten van verschillende communicatieomgevingen en gebruikersapparaten zoals telefoontoestellen, GSM's, smartphones, tablets en PC's.
Tegelijkertijd heeft elke organisatie noodzakelijkerwijs de weg ingeslagen om te komen

0THEMA10CYBER0010C01011000Y1010B0101E0011OR01TH01E01M001A1CY1010B00001B1100010ER10010100

van de vele ICT-keuzemogelijkheden naar een beheer(s)bare werkplekomgeving via de standaardisatie van functionaliteit. Het gaat dan vooral om de minimalisatie van de diversiteit aan communicatiemiddelen per gebruiker en per organisatie inclusief een efficiënte en effectieve inrichting van de werkplek. Standaardisatie van de nieuwe functionele mogelijkheden zal leiden tot een nieuwe inrichting van werkplekken die niet langer zijn gebaseerd op techniek of het hierarchische niveau van gebruikers in een organisatie, maar op effectiviteit voor de bedrijfsprocessen.

IP is als communicatiebasis een natuurlijke ontwikkeling, die voor alle mogelijke media van toepassing wordt, of al is.

Veranderend netwerkgebruik

Het internetgebruik is door de jaren heen sterk veranderd. In eerste instantie was het zoeken via webbrowsers, e-mail en toegang tot webhosting. De laatste jaren is het sterk gericht op de sociale netwerken en internettelefonie. Instant messaging, internet-shopping, muziek en video downloaden zijn de populairste activiteiten. Dat is de top aan toepassingen, voor zover je dat eigenlijk toepassingen mag noemen. Hierbij is in de periode 2001 tot 2008 het gebruik van internettelefonie de sterkste groeier. In de bedrijfsomgeving maakt ongeveer zeventig procent van de aansluitingen gebruik van een internettelefonietoepassing. Dat kan een VoIP-systeem lokaal zijn, of een ´hosted´ dienst. Daarnaast is in die jaren het aantal online Skype-gebruikers elk jaar verdubbeld. Inmiddels zijn er in de piek ongeveer dertig miljoen gebruikers online. Deze communicatiefaciliteiten zijn eigenlijk meer de basisinfrastructuur om in de internetomgeving verder te kunnen. Juist nu breedbandinternet in aantal aansluitingen wijd verspreid is en nog steeds groeit, biedt een dergelijke basisinfrastructuur goede mogelijkheden om interessante toepassingen snel uit te rollen. Dat wordt veroorzaakt door het grote aantal aansluitingen waardoor de 'killerapplicatie' een toepassing is die zeer snel in de markt zijn weg zal vinden. Juist door het grote aantal breedbandinternet-aansluitingen is dat een eenvoudige en goedkope distributiemethode. Wat zijn de interessante toepassingen? Daar is geen recept voor te geven, want het hangt af van de kernactiviteiten van de organisatie en de bedrijfsdoelstellingen en de uitwerking daarvan. Inmiddels zijn veel gebruikte toepassingen eenvoudig te achterhalen in elke app-store. In essentie kan het internet en dus elke IP-infrastructuur alleen maar maximaal ten diensten van de gebruikers staan als er sprake is van netneutraliteit. Het netwerk doet dan hetzelfde voor iedereen en doet hetzelfde voor elke toepassing.

Toepassingen en afhankelijkheid

Toepassingsgerichte e-mail

De toepassingsgerichte e-mail is gericht op een doelgroep (social media) of een bijlageuitwisseling en synchronisatie van bestanden. Een deel van het succes van dit soort toepassingen zit in de goede integratie met de desktop en mobiele gebruikersapparaten, waardoor ze allemaal over dezelfde informatie beschikken.

Social media communicatie (SMC)

Enkele zeer bekende voorbeelden met de bijbehorende doelgroep zijn:

- LinkedIn: zakelijk netwerk inclusief communicatiediensten.
- Facebook: persoonlijk gerichte communicatie op consumentenmarkt.
- Twitter: korte berichtendienst voor consumenten en zakelijke gebruikers.
- Yammer: als Twitter, maar dan binnen bedrijven en organisaties.
- Hyves: vergelijkbaar met Facebook, maar dan sterker gericht op consumentenmarkt

Bestandsuitwisseling

- Dropbox: mappen delen door verschillende apparaten of gebruikers.
- Mobile-me: synchronisatie van de desktop over apparaten of systemen.
- Yousendit, wetransfer, sendspace: uitwisseling van bestanden.

Een aantal van die diensten zijn, net zo als Skype indertijd, gericht op de consument, eenmansbedrijven of de zeer kleine bedrijven. Het gevolg van het neerzetten van deze diensten in de consumentenomgeving is, dat die consumenten vaak ook werknemer zijn bij grote bedrijven en vanuit die hoek in hun bedrijf gaan vragen om dit soort diensten. Op die manier wordt er een weg voorbereid om van consumentendiensten te gaan naar volledige clouddiensten. Wat dat betreft is er ook op applicatieniveau een vergelijk te maken met de diensten die bijvoorbeeld via Google docs geboden worden.

DE ONOMKEERBARE WEG

Integratie op technisch, functioneel en toepassingsniveau

De techniek heeft er voor gezorgd dat ICT-middelen meer functies hebben gekregen die voor meer *effectiviteit en efficiëntie* in de bedrijfsprocessen gezorgd hebben. Ook heeft er een verschuiving plaatsgevonden van *specifieke hardware* naar *generieke hardware*. Daarnaast is er sprake van een functionele integratie ('1+1=3 effect') die overigens nog lang niet ten einde is. Sensoren bieden namelijk nieuwe informatie en dus ongekende mogelijkheden. Ook is er een scala aan signaalconversiefuncties, aangestuurd door software, gekomen. Nieuwe types sensoren worden met regelmaat toegevoegd aan gebruikersapparaten. Het gaat dan om bijvoorbeeld GPS, (positiebepaling, maar ook positieverplaatsing), statische en dynamische camerabeelden, korte afstandscommunicatie (NFC, Near Field Communicatie) en gyroscoopgegevens voor apparaat-oriëntatie, maar ook bijvoorbeeld CO2 meting, hartslag of andere directe omgevingsgegevens. Verschillende typen sensoren maken het in combinatie met de software mogelijk dat nieuwe sensor overschrijdende combinaties beschikbaar komen. In de nabije toekomst zijn er ook sensoren te verwachten die informatie bieden over luchtkwaliteit, radioactiviteit, UV-intensiteit en andere omgevingscondities.

Op softwareniveau is er enerzijds een ontwikkeling die het mogelijk maakt om eenvoudigere toepassingen voor de verbetering van de bedrijfsprocessen te ontwikkelen en anderzijds is er software die makkelijker inzetbaar is voor de gebruiker. Het is een trend om er voor te zorgen dat de volgende generatie softwareversies de hardware nog beter voor de gebruiker benut. Deze vorm van upgrading maakt dat de gebruiker het gevoel heeft dat zijn hardware geen 'geïntegreerd verouderingsproces' in zich heeft.

Technologie en gevolgen

Er is een aantal technologieën die direct gevolgen hebben voor de data die er zich in bevinden. Het zijn alle industrie gedreven ontwikkelingen. Om het gevolg van die technologieën te kunnen overzien zal er beknopt op ingegaan worden. Wat zijn de belangrijkste technische elementen die de kwetsbaarheid van de data infrastructuur vergroten:

- virtualisatie;
- gebruiker, beheer en besturing op afstand in combinatie met connectiviteit;
- verclouding van data en
- smartphones, geïntegreerd in (overheids) beslisstructuren.

Virtualisatie

Virtualisatie is het draaien van verschillende, of meer bedrijfssystemen op één gemeenschappelijk hardware-platform. In de data- en telecomwereld is virtualisatie de laatste jaren, maar vooral de komende jaren, een belangrijke mogelijkheid om tot een efficiënte organisatie van de ICT-middelen en de communicatie-infrastructuur te komen. Deels komen de virtualisatiemogelijkheden doordat systemen met meer processoren tegelijkertijd kunnen werken. Dat geeft een bepaalde stabiliteit in performance en doorvoersnelheid van een ICT-systeem per proces dat op eenzelfde processor draait. De processen kunnen elkaar in een multicore omgeving niet meer zo in de weg zitten als in single core-systemen. Realtime, bijna realtime-systemen en systemen met een tijdgelimiteerde response hadden hier in het verleden echt last van, omdat de verwerkingstijd en daardoor de responsetijd varieerde. Virtualisatie maakt het mogelijk dat

0THEMA10CYBER00010C01011000Y1010B0101E00110R01TH01E01M001A1CY1010B00001B1100010ER10010100

verschillende toepassingen op één systeem onder verschillende bedrijfssystemen kunnen werken of dat verschillende toepassingen elk in hun eigen omgeving (vrijwel) onafhankelijk van de andere toepassingen kunnen werken. De sterk toegenomen hardware-performance in combinatie met meer processorkernen maakt de virtualisatie mogelijk. Daarnaast is de multi-core ontwikkeling van belang om beter tegemoet te komen aan realtime-performance. Processen zijn aan een verschillende processorkern toewijsbaar en dat maakt dat de realtime-performance van een toepassing beter voorspelbaar is geworden.

De virtualisatieslag zorgt er voor dat er minder hardware en dus ook minder systemen nodig zijn

Gebruiker, beheer en besturing op afstand in combinatie met connectiviteit

Er is een toenemend aantal functies die het mogelijk maakt allerlei vormen van filetransfer en files gemeenschappelijk te delen, te gebruiken op een manier dat ze ook nog eens opslag 'elders' verzorgen. De mate van integratie met de desktop en synchronisatie tussen verschillende desktops, laptops tablets of smartphones maakt het gebruik van cloud computing steeds makkelijker en vaak ook verleidelijker door het gebruikersgemak wat ze bieden. Op vrij korte termijn zullen de cloudfuncties invloed hebben op zowel de toepassingslaag als de gebruikersapparatuur.
'Informeer een ander en er is meer gratis opslagruimte', is een variant waarmee Skype de markt veroverde. Een voorbeeld van synchronisatie via opslagruimte is Dropbox.

Verclouding van de data

Waar de datadragers 'all over the world' staan, is niet meer duidelijk voor de eigenaar van de gegevens. Dat ze er zijn ja, maar waar de data zich fysiek bevinden is geheel niet meer duidelijk. De vragen die daarbij aan de orde komen zijn verschillend. Voor de consumentenomgeving of voor de bedrijfsomgeving zijn er voor hetzelfde punt verschillende invalshoeken. Vanuit de consumentenhoek passen er meer vragen bij in de richting van de privacy van de informatie, ook in relatie tot de eigenaar van de gegevens. Vanuit de bedrijfsomgeving zijn de vragen meer gericht op veiligheid, integriteit, beschikbaarheid, bereikbaarheid en continuïteit van de informatie:
- Wie kan de informatie nog meer zien?
- Kan ik altijd bij mijn informatie?
- Is er een kans dat ik er niet meer bij kan?

Wanneer de digitale gegevens buiten de landsgrenzen bewaard zouden worden, zijn er wellicht nog andere wetten en regels die er gelden dan in het land waar de data vandaan komt. Sterker nog, wat gebeurt er als een buitenlands bedrijf de cloud-diensten nationaal aanbiedt? Is er dan regelgeving die dat buitenlandse bedrijf door hun eigen overheid opgelegd heeft gekregen en daardoor invloed kan hebben op de data of de inhoud van de data?
Het zijn, door het begin van het cloudtijdperk en dus gebrek aan ervaring, nog onbeantwoorde vragen die wel van cruciaal belang zijn voor de continuïteit van de bedrijfsprocessen van de eigen organisatie:
- geen IP-connectie: geen data,
- geen data: de bedrijfsprocessen komen tot stilstand,
- stilstand: op enig moment niet meer in te lopen schade,
- of uiteindelijk nog erger.

Cloudcomputing is ook niet zonder risico voor de feitelijke informatie-inhoud. Het vergt een principiële afweging, temeer daar hardware kosten en de prijzen van datadragers nog steeds dalende zijn in een markt waar tegelijkertijd de ICT-capaciteit ook nog steeds stijgt. De financiële noodzaak neemt dus af om iets buiten de deur te hebben, tenzij men van een investeringsgerichte infrastructuur naar een dienstverleningsbetalingsstructuur, exploitatiekosten wil komen. Cloudcomputing is verleidelijk, echter het afbreukrisico versus de gevolgen van: geen bedrijfsgegevens meer ter beschikking hebben, is een grondige evaluatie waard.

De cloud, het klinkt zo goed, alle problemen zijn opgelost. In datzelfde kader wordt de keuze iets eenvoudiger als de data nationaal in plaats van internationaal bewaard worden. Ook is er natuurlijk een beveiligingsprobleem. Gaat er iets fout met de toegangscontrole bij clouddiensten als Mobileme/iCloud en Dropbox dan zijn alle gegevens zichtbaar. Een ander punt van aandacht is dat alle data in theorie inzichtelijk is voor de datacenter eigenaar of wellicht zelfs de overheid in dat land wanneer de gegevens er onvercijferd, of onvoldoende sterk vercijferd zijn opgeslagen. Op dat punt is de regelgeving echt per land verschillend. Er zijn clouddiensten, die er vercijfering bij leveren, ook op basis van het bekende en veilig geachte AES-256. De vraag is echter hoe het sleutelbeheer ingericht is en of de cloudbeheerder daar bij kan, maar ook of dit een vercijferingsmechanise is zonder backdoorconstructie. Daar ligt namelijk de kern om van de bitjes weer informatie te maken. Gezien de eisen die de Patriot Act aan VS cloudbeheerders stelt is te verwachten dat die daar wel bij kunnen. In dat geval, maar eigenlijk in alle gevallen is het beter om zelf de vercijfering van de eigen data te organiseren en te beheren.
De dienstverlening vanuit de cloud, bijvoorbeeld hosted VoIP of hosted videoconferencing is vaak minder gevoelig dan het verlies van de complete data- en informatievoorziening die in de cloud is van een bedrijf. In een VoIP–systeem worden bijvoorbeeld geen gesprekken opgeslagen. De informatie is er alleen maar gedurende het transport.
Hosted VoIP is een trend waarbij kleine bedrijven zich ontdoen van de eigen fysieke infrastructuur. De reden hiervan is de flexibiliteit van de dienstverlening, de meer korte termijn van de business en het gebrek aan beheer(s)kennis in de kleinere omgevingen. In die kleinere omgevingen is het percentages GSM's relatief hoog waardoor er een vorm van een 'Plan B' is.

Smartphones, maar dan inmiddels geïntegreerd in overheidsbeslisstructuren

De verschuiving in toepassing van een smartphone van back-up medium voor de werkplek naar het mobiele werkplekapparaat is gaande. De volgende verschuiving zal zijn dat het apparaat onderdeel van het werk en dus van bedrijfsbeslisstructuren wordt. Die verschuiving veroorzaakt dat uitval van de hosting infrastructuur een serieus bedrijfsrisico aan het worden is. Tot voor kort werd er gedacht dat de werkplek tenminste nog wel een soort back-up van het mobiele apparaat voor de werkcontinuïteit zou zijn. De smartphone wordt daardoor niet alleen de primaire werkomgeving. Het gaat in snel tempo verder: de vaste plek zal door de toenemende mogelijkheden geminimaliseerd worden of verdwijnen. Voor veel gebruikers zal de smartphone onderdeel worden van het primaire bedrijfsproces en dus van beslisprocessen. De oude bedrijfsprocessen, papier en post, verdwijnen en is voor de minsteriele top met het gebruik van de Black Berry al lang het 'point of no return' gepasseerd, omdat de apps van de smartphone of tablet de communicatie en daarmee de bedrijfsprocessen zo enorm versnellen en plaats onafhankelijk gemaakt hebben. Maar als de hosting locatie van RIM (Black Berry uitvalt), vertraagt en stopt dit beslisprocessen van menig organisatie.
Hiermee wordt de uptime van het hosting netwerk en de wijze waarop die in elkaar vervlochten zijn met de gebruikersapparaten op zijn minst interessant en uiteindelijk cruciaal. Wat werkt er allemaal niet bij uitval van de hostingomgeving, die heel ergens anders staat. Is het de e-mail pushservers die niet meer werken, maar doet het internet het nog, is Facebook, LinkedIn of Twitter niet meer bereikbaar? Hoe en waarmee is het medium in beslisprocessen allemaal mee geïntegreerd? Een 'last minute' afspraakwijziging gaat bijvoorbeeld al fout bij uitval van de agenda smartphone functie: de gehoste agendafunctie. Het zal duidelijk zijn de verder gaande migratie naar smartphones en tablets en de daar opvolgende integratie is onomkeerbaar geworden.
Tablets en smartphones hebben door de synchronisatiemogelijkheden alle gegevens

van de desktop in principe in zich. Dat betekent dat die gegevens net zo mobiel zijn als het apparaat zelf. Bedrijfsgegevens zijn dus veel buiten de deur en verlies is zo gebeurd.

Afgelopen jaren was 'USB stick' synoniem met 'laten rondslingeren' en datzelfde ligt in het verschiet voor de smartphone. Was de USB stick nog een datastick, de smartphone is de informatiestick.

Mensen, maar ook bedrijven, zetten direct of indirect veel bedrijfs- en persoonlijke gegevens in hun smartphone. Zij worden hierdoor kwetsbaar, zeker nu ook minder goed of onbeschermde smartphones en tablet-PC's gemeengoed aan het worden zijn. Diezelfde potentiële kwetsbaarheid geldt overigens ook voor informatie die medewerkers via de social media over zichzelf en hun bedrijf naar buiten uiten. Mocht de individuele informatie net interessant lijken, die van een groep of bedrijf wel zeker: macrodata, mega interessant.

Uitval van smartphone-hosting en de gevolgen
Het is bekend dat een hosting-infrastructuur zeldzaam uitvalt. Maar als die infrastructuur uitvalt, dan duurt die vrijwel altijd veel langer dan wanneer een dergelijke infrastructuur in eigen beheer is georganiseerd. Een infrastructuur in eigen beheer daarentegen valt dan wel weer vaker, zij het korter uit, dan een gehoste infrastructuur. Dit zijn constateringen in de markt. Niet onlogisch overigens, want hostinginfrastructuren zijn groot en ze bedienen een diversiteit aan organisaties die weer een veelheid aan locaties en gebruikers hebben, verspreid over landen en zelfs verschillende continenten. De hostingmiddelen van de smartphone-providers staan in goed geconditioneerde datacenters en zijn bereikbaar via diverse WAN-structuren van verschillende providers.
De eigen infrastructuur is echter altijd veel minder complex dan de hosting infrastructuur van de provider, want die eigen infrastructuur bedient maar één organisatie. Technisch gezien wordt er meestal ook maar één WAN doorlopen. De eigen infrastructuur is verhoudingsgewijs meestal weer minder degelijk gehuisvest dan die van de hostingproviders. Deze elementen maken het dat de eigen infrastructuur door de relatieve eenvoud minder lang uitvalt dan de veel complexere hosting infrastructuur.

(GEEN) TOEPASSINGEN EN WAT ZIJN DE GEVOLGEN?

Er is een groot aantal toepassingen waarvan er vele niet direct voor de ene, maar weer wel voor de andere gebruiker nuttig zijn. Ze hebben wat betreft smartphones alle echter gemeen dat ze de verwerkingskracht, sensorinformatie en identificatiemogelijkheden van gebruikers van de smartphone combineren met communicatieverbindingen met als resultante: toegevoegde waarde voor de gebruiker. Zonder communicatieverbinding is een smartphone of een tablet waardeloos. Het is geen apparaat voor standalone gebruik. Het spanningsveld is echter ook meteen daar.
Geen internet, dus:
- geen bruikbaar apparaat, dus
- geen deelname aan de bedrijfsprocessen, dus
- stagnatie in het werk, dus
- imagoschade, of
- bedrijfsschade, of
- erger: klantenverlies.

Anno 2011 zijn 3,5 miljoen smartphones verkocht in Nederland. De praktijk zal zijn dat menig bedrijf achterloopt op wat de werknemer meeneemt van thuis naar zijn werk. In verschillende bedrijven zal daarom snel een aanvulling op het communicatiebeleid moeten worden gemaakt, om het gebruik van smartphones en tablets te reguleren. De beveiliging van bedrijfsinformatie wordt hiermee direct relevant en zal eveneens opnieuw moeten worden gedefinieerd en ingevuld. Een uit te werken gebruikers- en beveiligingsbeleid, is rond het 'bring your own device' principe van essentieel belang. Dit brengt met zich mee dat er naast beveiliging en beheerondersteuning ook financiele aspecten zijn door het zakelijke en privégebruik in relatie tot de fiscus en vergoedingen van bedrijfswege voor het zakelijk gebruik van een privé-apparaat, of het privé gebruik van een zakelijk apparaat.

3. Enkele Incidenten in het nieuws van 2011
Onderstaand wordt een opsomming geven van enkele in het oog springende nieuwsfeiten, die de ongewenste toegankelijkheid en aanpasbaarheid van data illustreren en een indicatie geven van de maatschappelijke gevolgen. De incidenten zijn gerangschikt op basis van een nationaal of een internationaal element dat er in de hack zit.

Nationaal
1. De Diginotar-hack: overheidsinformatie voor derden toegankelijk en aanpasbaar, overheidsorganisaties konden onderling niet meer goed communiceren, evenals burgers naar die overheidsonderdelen
2. Diginotar-hack gevolgen. Door de hack zijn beveiligingscertificaten van getroffen websites niet veilig meer. Verkeer kan worden omgeleid en anderen kunnen meelezen. Gebruikers kunnen er niet langer zeker van zijn dat ze zich daadwerkelijk op de site bevinden waarvan het adres in de adresbalk van de browser staat.
3. Valse certificaten zijn behalve voor Gmail ook uitgegeven voor Twitter, Skype, Hotmail, Yahoo en Microsoft Messenger. Volgens de NOS wordt de maildienst van Yahoo veel gebruikt door Iraniërs in de oppositie.
4. IT beveiliging bedrijven, waaronder een Nederlands bedrijf verkopen spyware software (Wikileaks)
5. Lektober hacks, 30 tal opsomming van lekke websites, manipuleerbare websites, meestal in de overheidssfeer.
6. Het Britse Vodafone netwerk te hacken via femtocell, dit kan in Nederland ook….
7. Het Hof in Den Haag stelt dat het niet strafbaar is om mee te liften op het Wi-Fi-netwerk van anderen, ook niet als dat netwerk beveiligd is. Van computervredebreuk is geen sprake.
8. Diginotar-hack ondermijnt Windows Update, de gevolgen zijn dat de windowsupdate wat anders kan zijn en dus de pc infrastructuur kan gaan ontregelen.
9. Hack de Overheid strijdt voor meer transparantie bij de overheid en bouwt ICT-toepassingen om die informatie toegankelijk te maken voor het grote publiek. De organisatie wordt gedreven door een los netwerk van jonge ICT-experts, hackers en journalisten. Ze maken sites, zoals de zoekmachine Open KvK, waar 24 uur per dag gratis gegevens uit de Kamer van Koophandel zijn op te vragen, en Politwoops, waar de Twitterberichten van politici die zij zelf hebben verwijderd, terug te vinden zijn.

Internationaal
10. De sites van onder meer National Geographic, Vodafone, Acer en The Register leken dit weekend gehackt. De oorzaak lag bij een DNS-hack die bezoekers naar andere sites stuurde. Wie dit weekend naar een van de sites surfte kwam volgens beveiligingsbedrijf Sophos terecht op pagina's van Turkse hackers. De sites zelf zijn niet aangevallen, maar het DNS-systeem wel. DNS zorgt ervoor dat de naam van een bepaalde website, bijvoorbeeld www.zdnet.be, doorverwijst naar het IP-adres van de server waar de site op draait. Wie zo'n systeem kraakt, kan een domeinnaam in principe laten doorverwijzen naar elke server of website. DNS is de internet telefoongids en de basis voor wie is wie en niet wie is een ander dan ik denk.
11. De Chinese aanval op Google, Adobe en andere technologiebedrijven werd deels uitgevoerd met behulp van een nieuw lek in Internet Explorer. Dat heeft Microsoft zelf bevestigd.
12. De computerhack bij Diginotar heeft mogelijk ernstige gevolgen voor 300.000 mensen in Iran. Hun internetverkeer is gevolgd met behulp van cer-

0THEMA10CYBER00010C01011000Y1010B0101E00110R01TH01E01M001A1CY1010B00001B1100010ER10010100

tificaten die werden vervalst dankzij de hack bij het Nederlandse bedrijf.

Bedreiging van zwaar industriële omgevingen

13. Problemen in de Verenigde Staten. Het complete Amerikaanse elektriciteitsnetwerk blijkt geïnfiltreerd door Russische en Chinese "cyberspionnen". Regelmatig nemen de hacker-spies even een kijkje in de Amerikaanse elektriciteitskeuken. Of dat van het leidingwaternet. Of kerncentrales.
14. Vier hackaanvallen zijn in 2007 en 2008 uitgevoerd op Amerikaanse satellieten die worden ingezet voor observatie van klimaat en aarde. Dat schrijft persbureau Bloomberg op basis van een rapport van een Amerikaanse congrescommissie dat volgende maand verschijnt.
15. Volgens een artikel in de Britse krant The Guardian worden de veiligheidsmaatregelen van Britse kerncentrales verscherpt nadat een bewakingsagent probeerde het computernetwerk van een nucleaire installatie in Bradwell, Essex, dicht bij Londen, te hacken. De pogingen van de man om in te breken in het netwerk en gevoelige informatie te verwijderen, slaagden en veroorzaakten een alarmsituatie in de centrale, waardoor alle deuren automatisch op slot gingen.

Naar aanleiding van deze punten:
In essentie heeft vrijwel elke hack een directe negatieve impact voor één of meer organisaties in Nederland en het merendeel van deze activiteiten kunnen, omdat IP-communicatie afstandsonafhankelijk is, letterlijk dus grenzen-loos. Ook is er geen 'firewall' voor ongewenste, onbedoelde zaken die van (ver) buiten de landsgrenzen gebeuren.

TOT SLOT

De voorgaande punten zijn maar een kleine greep uit het 2011 nieuws in de media. In essentie betekent dit dat er met kennis of een equivalent daarvan (geld…), mogelijk is om data te vergaren, data te manipuleren en dus organisaties te beïnvloeden. Kennis is geld en geld is concurrentie of het equivalent uiteindelijk ervan macht, Inmiddels kan dat dankzij IP als communicatiebasis dus op afstand en zonder 'op bezoek te komen', zonder fysieke sporen achter te laten gebeuren, zelfs vaak zonder logische sporen achter te laten.

Er zijn overheidsorganisaties, die voor zich zelf druk bezig zijn of zijn geweest om hun eigen informatie te beveiligen. Dat geldt echter voor hun zelf, maar niet vanuit hun kennis van en voor de overheid, vooral voor Nederland BV, terwijl deze bovenstaande adhoc nieuwsselectie juist aangeeft dat buiten een select deel van de overheid de netwerkinformatiebeveiliging voor Nederland bv mis gaat en mis zal blijven gaan.

In de afgelopen jaren is de communicatie-infrastructuur van een fysieke infrastructuur met fysieke bescherming overgegaan naar een elektronische infrastructuur gebaseerd op data transport en inmiddels op basis van IP-transport, voor elke communicatie toepassing.

Al heel lang is er fysieke bescherming voor Nederland BV, zoals Politie en Defensie. Echter de doorvertaling van de fysieke beveiliging van toen naar de beveiliging van de logische communicatie en informatiestructuur van nu, mist bij de overheid en daarmee ontbreekt de cruciale inbreng voor de bescherming van de communicatie-infrastructuur, want die is wel enige tijd geleden van fysiek naar logisch overgegaan. Het is dus niet een nieuw Nationaal Noodnet aanleggen, dat is een oplossing voor een geheel ander probleem.

Door de integratie van IP in alle communicatietoepassingen is de netwerkinfrastructuur en de toegang er toe essentieel en cruciaal geworden voor de bedrijven en organisaties waar Nederland BV uit bestaat. Die individueel en als totaal bijzonder kwetsbaar en zelfs manipuleerbaar, zijn geworden en waar geen collectieve bescherming (nog) tegenover staat.

BRONNEN:

- **www.otmc.nl**
- Delen van dit artikel zijn ontleend aan het boek: Communicatie-infrastructuren, het primaire bedrijfsproces; verschijningsdatum januari 2012
- **www.communicatie-infrastructuur.nl**