I/O VIVAT

JAARGANG 28
NUMMER 2

Narrowcasting: Schermen overal
Altijd en overal informatie

TREsPASS
Informatie beter beveiligen met scenario's

Anatomie van een Pentest
Kijken door de ogen van een hacker

Cybersecurity
Wat doet Nederland om haar digitale landsgrenzen te verdedigen?

Een reis door Azië
Met Inter-Actief door Zuid-Korea en China

En verder...
KPN Consulting
Op bezoek bij Topicus
Trends & Hypes: NFC
Van de voorzitter
Van het ENIAC-bestuur
Op bezoek bij Shell
Turing Award-winnaar in beeld
Van Rom

Inter-Actief

ADVERTENTIE

VI_IMAGO_ADV_A4_STAAND

//Colofon

Jaargang 28, nummer 2,
Februari 2013
ISSN: 1389-0468

I/O Vivat is het populair-wetenschappelijke tijdschrift van I.C.T.S.V. Inter-Actief, de studievereniging voor Technische Informatica, Bedrijfsinformatie-technologie en Telematica van de Universiteit Twente. I/O Vivat verschijnt vier maal per jaar en heeft een oplage van 1700 exemplaren.

// Hoofdredactie
Herman Slatman

// Redactie
Michel Brinkhuis, Ralph Broenink, Rick van Galen, Ronald Meijer, Niek Tax, Stijn van Winsen

// Vormgeving
Niels Witte

// Gastschrijvers
Willem de Boer, Harald Dannenberg, Pim Jager, Rom Langerak, Johan Noltes, Rianne Honhoff, Arnold van Mameren, Wolter Pieters

Voor vragen, suggesties en tips is I/O Vivat bereikbaar via e-mail op vivat@inter-actief.net, twitter op @iovivat, telefonisch op 053-489 3756 of per post:
Studievereniging Inter-Actief
Postbus 217
7500AE Enschede

De studievereniging wil de adverterende bedrijven bedanken voor de samenwerking.

// Drukwerk
Drukkerij van den Bosch & Fikkert

© 2013 I.C.T.S.V. Inter-Actief

I/O VIVAT

//Redactioneel

Groeiende internationalisering en globalisering is een overduidelijk onderdeel van de huidige samenleving, en misschien wel in het bijzonder op het gebied van alles wat met informatica en ICT te maken heeft. Nieuws van de andere kant van de planeet bereikt ons in no-time en bevriend raken met bijvoorbeeld een Chinees is zo gepiept. En dat allemaal dankzij het Internet dat ons tegenwoordig met van alles verbindt. Het Internet is echter niet enkel goeds, want er ontstaan ook nieuwe dreigingen waarop ingespeeld moeten worden.

Zo werd in Den Haag begin dit jaar de Taskforce Cyber opgericht, onder aanvoering van kolonel Hans Folmer, die in de wandelgangen bekend staat als de cyber-kolonel. Internationale samenwerking, in een periode waarin digitale dreigingen realiteit kunnen worden, is bij de aanpak van deze bedreigingen van groot belang, aldus Folmer. Het delen van kennis op internationaal gebied is essentieel, omdat dreigingen niet langer enkel uit eigen land hoeven te komen. Cyber is het vijfde domein in oorlogsvoering geworden.

Een ander voorbeeld van het internationale aspect van informatica is het werken bij internationals of het te werk gesteld worden op buitenlandse locaties. Dit is bijvoorbeeld het geval voor Rianne Honhoff, werkzaam bij Shell. Zij vond het internationale aspect van Shell één van de belangrijkste prikkels om juist bij Shell te gaan werken. Haar verhaal is verderop in deze I/O Vivat te lezen.

En dan was er natuurlijk ook nog Noodle, de studiereis van Inter-*Actief*, die dit jaar de landen China en Zuid-Korea aandeed en als thema IT Integrated Lifestyle droeg. Waar anders dan in Seoul, Zuid-Korea, waar de hele samenleving doordrenkt is van techniek en modern design, komt dit thema beter tot zijn recht. Lees er verderop meer over!

Ik wens je veel leesplezier met deze 'internationale' I/O Vivat!

Herman Slatman
Hoofdredacteur

//Inhoud 28.2

topicus

kpn consulting

Technolution

//Nieuws

Onderzoekers verklaren pixel 'bijna-dood'

Een team van onderzoekers van de Universiteit van Bath, Root6 Technology, Smoke & Mirrors en Ovation Data Services ontwikkelen een videocodec op basis van vectoren. Deze zou volgens het team op vrij korte termijn kunnen leiden tot een einde aan de pixel.

Traditionele video-codecs maken gebruik van pixelinformatie in een video. Hoe meer pixels per frame, des te duidelijker en scherper zal de video zijn. Het nadeel hiervan is dat wanneer er gebruik gemaakt wordt van een grote hoeveelheid pixels er een zeer grote hoeveelheid data ontstaat. Codecs worden gebruikt om deze hoeveelheid data enigszins te verkleinen.

Zodra normale afbeeldingen geschaald worden vindt er stretching van pixels plaats. Deze zien er niet scherp meer uit en de afbeelding wordt er lelijk van. Om dit tegen te gaan werden vectorafbeeldingen ontwikkelt. Deze schalen in principe oneindig zonder dat er verlies van kwaliteit plaatsvindt. Codecs die gebruikmaken van vectorafbeeldingen bestonden er echter nog niet.

De nieuwe ontwikkeling zal volgens professor Phil Willis leiden tot een revolutie in de manier waarop digitale media geproduceerd en geconsumeerd wordt. Door gebruik te maken van de nieuwe codec kan een film haarscherp afgespeeld worden in ieder gewenst formaat.

Het team is nog op zoek naar andere spelers in de markt die een duit in het zakje willen doen. Een demo is al wel te zien op http://www.cs.bath.ac.uk/vsv/

Prof. Apers wint ICT Personality Award 2012

De Nederlandse ICT-brancheverenging Nederland ICT, sinds 14 december de nieuwe naam van ICT~Office, heeft de jaarlijkse ICT Personality Award prijs uitgereikt aan Prof. Dr. P.M.G. (Peter) Apers en Prof.Dr.Ir. A.W.M. (Arnold) Smeulders. Deze prijs is hen uitgereikt wegens hun gezichtsbepalende rol voor het ICT-onderzoek in Nederland. Apers leverde samen met Smeulders een belangrijke bijdrage aan de ICT Roadmap voor alle topsectoren binnen het topsectorenbeleid van de Nederlandse overheid.

De roadmap geeft prioriteiten en onderwerpen aan voor fundamenteel en toegepast ICT-onderzoek en de agenda voor ICT-innovaties. Sinds 1985 is Apers hoogleraar aan de Universiteit Twente in Databases. In 2002 is Apers benoemd tot wetenschappelijk directeur van onderzoeksinstituut CTIT aan de Universiteit Twente. Onder leiding van Apers als wetenschappelijk directeur groeide het CTIT uit tot een van de grootste academische instituten in ICT-research binnen Nederland. Tevens is Apers directeur van het 3TU Netherlands Institute for Research on ICT (3TU.NIRICT), de overkoepelende organisatie voor al het ICT onderzoek binnen de drie Nederlandse technische universiteiten.

Eerdere winnaars van de ICT Personality Award zijn onder andere Jan Kees de Jager en Raymond Spanjar.

Bron:

http://www.nederlandict.nl/index.shtml?id=12447&ch=ICT

http://www.utwente.nl/archief/2012/12/ict_personality_award_voor_ut_wetenschapper_prof._peter_apers.doc/

http://www.computable.nl/artikel/nieuws/loopbaan/4616188/1458016/nederland-ict-reikt-personality-award-2012-uit.html

DARPA wil 100 gbps draadloze netwerkapparatuur realiseren

Ondanks alle ontwikkelingen in de industrie om snellere draadloze netwerken mogelijk te maken, blijven de behaalde bandbreedtes ver achter bij bekabelde netwerken. Glasvezel vormt in de huidige civiele en militaire netwerken de kern van het netwerk.

Het onderzoek van DARPA is in de eerste plaats vooral gericht op gebruik van draadloze netwerken in omgevingen waar snel een netwerk opgezet moet worden voor militaire doeleinden. en waar het misschien onmogelijk is om een bedraad netwerk neer te leggen. In het verleden zou dit leiden tot het gebruik van alternatieve communicatiemethoden die als nadeel hebben dat er een lagere data-rate beschikbaar is voor de operationele eenheden. Het 'online' bekijken van de videofeed van een Unmanned Aerial Vehicle is dan bijvoorbeeld één van de dingen die moelijker wordt.

Het doel van het onderzoek is om apparatuur te ontwikkelen die gebruikt kan worden om een 100 gigabits per seconde draadloze datalink te realiseren over afstanden tot 200 kilometer. Het grootste probleem hierbij is dat er geen gebruik gemaakt kan worden van optische signalen, aangezien wolken de ontvangst dan in de weg zitten. Er zal dus gebruik gemaakt moeten worden van radiosignalen. Technische ontwikkelingen in de modulatie van millimetergolflengtefrequenties zouden draadloze snelheden tot 100 gbps mogelijk moeten maken.

De uitdaging ligt volgens Dick Ridgway bij het efficiënt gebruikmaken van het beschikbare deel van het radiospectrum en om apparatuur te ontwerpen die uiteraard goed functioneert, maar daarnaast ook voldoet aan specifieke eisen aan grootte, gewicht en energieconsumptie. Hoewel het onderzoek dus vooral op militaire toepassingen gericht is, zouden doorbraken in dit gebied echter ook hun weg kunnen vinden naar commerciële toepassingen, zoals in het verleden wel vaker is gebeurd.

Bron: http://www.darpa.mil/NewsEvents/Releases/2012/12/14.aspx

Kwart van de Europeanen zonder internet

Eurostat, het statistisch bureau van de Europese Unie, heeft op 18 december een rapport uitgebracht over internet toegang en gebruik binnen de Europese Unie. In dit rapport valt te lezen dat net iets meer dan driekwart van alle huishoudens binnen de 27 landen van de Europese Unie toegang hebben tot internet. Bulgarije (51%), Griekenland (54%), Roemenië (54%) laten de laagste cijfers van internettoegang zien. Kandidaat-lidstaten Montenegro (55%) en Turkije (47%) noteren echter ook lage percentages in huishoudens met internettoegang. Positief lijkt dat de landen die lager scoren op internettoegang vaak wel die landen zijn die ten opzichte van de vorige meting in 2009 de meeste vooruitgang laten zien. Naast internettoegang zijn ook de toegangscijfers tot breedbandinternet in het rapport meegenomen. Qua toegang tot breedbandinternet scoort Nederland (83%) vierde binnen de EU, direct achter Zweden (87%), Finland (85%) en Denemarken (85%). Kandidaat-lidstaat IJsland laat echter het hoogste percentage toegang tot breedbandinternet zien met 91%.

Naast toegangscijfers onderzocht Eurostat ook waarvoor internet wordt gebruikt. Afhandelen van e-mails en het vinden van informatie behoren tot de activiteiten die onder internetgebruikers in de hele EU het meest worden gedaan (89% en 83% respectievelijk). Andere noemenswaardige conclusies zijn het percentage internetgebruikers die posten op sociale media, die in Portugal met 75% bijna dubbel zoveel is vergeleken met het Europees gemiddelde. In Nederland en Hongarije zijn met 17% respectievelijk 16% de hoogste percentages gemeten van internetgebruikers met een eigen website of blog, deze percentages liggen ruim tweemaal hoger dan het Europees gemiddelde.

Bron: Eurostat report 'Internet access and use in 2012'

Bron: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-18122012-AP/EN/4-18122012-AP-EN.PDF

Videogame gecreëerd door kunstmatige intelligentie

Normaal gesproken komt het verband tussen kunstmatige intelligentie en games voornamelijk naar voren in het feit dat er in games vaak gebruik gemaakt wordt van computergestuurde tegenspelers.

Michael Cook, een PhD onderzoeker aan het Imperial College in London, geeft echter een heel andere draai aan bovenstaand feit. Hij ontwikkelde ANGELINA – A Novel Game-Evolving Labrat I've Named ANGELINA – een systeem dat gebruik maakt van kunstmatige intelligentie om games te produceren.

ANGELINA maakt gebruik van games die eerder geprogrammeerd zijn om automatisch games te creëren, maar heeft hierbij wel assistentie van mensen voor nodig. Zo moeten het spelkarakter, een doel en obstakels van te voren gegeven zijn. ANGELINA gebruikt daarna elementen uit andere games om van deze gegeven objecten een game te produceren. Zo kijkt ANGELINA hoe een probleem in een andere game opgelost moet worden: hoe komt een speler in game X voorbij dit obstakel. Dit proces wordt een aantal maal herhaald om verschillende gamelevels, en daarmee een volledige game te produceren.

Cook is van mening dat gamedevelopers, en dan met name programmeurs, niet bang hoeven te zijn dat hun werk overgenomen zal worden door computers. Hij voorziet een wereld waarin programmeurs en systemen als ANGELINA samen kunnen werken om nieuwe ideeën en mechanieken te ontwikkelen. Het concept is daarnaast niet slechts op het programmeren van games van toepassing, maar draagt daarnaast ook bij aan kunstmatige intelligentie in het algemeen.

De eerste volledig door ANGELINA ontwikkelde game is 'A Puzzling Present', is beschikbaar voor Windows, Mac, Linux en Android en is gratis verkrijgbaar op http://www.gamesbyangelina.org/

Bron: http://phys.org/news/2012-12-phd-student-ai-machine-video.html

Mobiele browsers 'blijken' onveilig

Onderzoekers van het Georgia Institute of Technology onderwierpen tien browsers voor mobiele apparaten, die tezamen een marktaandeel van 90% hebben, aan een onderzoek om vast te stellen of deze aan de gebruiker aangeven of zij te maken hebben met een veilige of onveilige website. Hun conclusie luidde dat geen enkele browser een indicatie gaf van mogelijke onveiligheden.

Browsers op desktops hebben tegenwoordig de beschikking over SSL-indicatoren, die gebruikt worden om aan te duiden dat een gebruiker op dat moment verbindt met een server via HTTPS. Deze zijn meestal te herkennen aan het karakteristieke slotje of een groen vak in de adresbalk. Hoe deze indicatoren weergegeven moeten worden, is door W3C vastgesteld.

De tien onderzochte browsers blijken niet over deze SSl-indicatoren te beschikken, waardoor gebruikers niet in staat zijn om vast te stellen of zij te maken hebben met servers die gebruikmaken van SSL om hun content te leveren. De mobiele browsers voldoen daarmee niet aan de aanbevelingen van de W3C.

De belangrijkste reden voor de afwezigheid van de SSL-indicatoren is volgens de onderzoekers dat er op mobiele apparaten over het algemeen minder ruimte is om informatie weer te geven. Bij het design van de browsers is er geen rekening gehouden om een plaats te geven aan deze SSL-indicatoren, waardoor ze nu ontbreken. Gebruikers van mobiele browsers zouden door het ontbreken van deze indicatoren eerder op onbetrouwbare websites terecht kunnen komen. Dit in combinatie met het groeiende aantal malware dat beschikbaar komt voor mobiele apparaten zou kunnen resulteren in een zeer groot infectiepercentage.

Bron: http://phys.org/news/2012-12-mobile-browsers-safety.html

Shell

Interview met Rianne Honhoff

Door: Rianne Honhoff
IM/IT Program manager voor Capital Projects

Rianne studeerde tussen 1999 en 2005 BedrijfsInformatie Technologie (BIT) aan de Universiteit Twente. Inmiddels is ze getrouwd, heeft ze een kind en is ze in verwachting van de tweede. Ze woont in Rijswijk, waar ze nu ook al zeven jaar werkt voor Shell.

Hoe ben je na je studie bij Shell terecht gekomen?

De belangrijkste reden dat ik voor Shell gekozen heb, is eigenlijk dat mijn beide ouders ook in de IT bij Shell gewerkt hebben. Ik heb zo veel goede verhalen meegekregen over het bedrijf. Voor hun werk hebben mijn ouders, en ik dus ook, een tijd in Oman gewoond. Dat was een hele bijzondere ervaring; het werken bij een internationaal bedrijf leek mij dan ook wel wat. Ik heb mijn afstudeerstage bij Philips afgerond, maar de bedrijfscultuur daar paste niet helemaal bij me. Om bij Shell aangenomen te worden heb ik deelgenomen aan de Shell Gourami Business Challenge, heb ik stage gelopen bij de NAM in Assen, dat een joint venture is van Shell, en heb ik deelgenomen aan een assessment center bij Shell.

Wat voor werk doe je momenteel bij Shell?

Op dit moment ben ik IM/IT Program Manager voor Capital Projects. Capital Projects is een onderdeel van Shell dat zich bezighoudt met de grotere business projecten, bijvoorbeeld het bouwen van een nieuwe raffinaderij of de ontwikkeling van een olieveld. Mijn huidige project is de ontwikkeling van een olieveld in de Noordzee dat 40 jaar geleden ontdekt is, maar toen niet rendabel was voor het bedrijf, nu in zeer korte tijd te realiseren aangezien de licentie op het olieveld binnenkort verloopt. Mijn rol als IM/IT Program Manager houdt in dat ik alle informatiemanagement en informatietechnologie voor, tijdens en na het project in goede banen leid. Op het gebied van informatietechnologie houdt dit bijvoorbeeld in dat ik bij de opzet van een nieuw kantoor er zorg voor draag dat alle laptops, applicaties en dataverbindingen beschikbaar zijn. Op het gebied van informatiemanagement houdt mijn rol in dat ik ervoor zorg dat er tijdens het project goed gedocumenteerd wordt, en dat de documentatie goed beheerd wordt. Dit doe ik uiteraard niet allemaal zelf; ik heb een coördinerende rol en ik maak dan ook vooral gebruik van bestaande afdelingen binnen Shell.

Wat vind je leuk aan het werken bij Shell?

Ik vind het leuk om samen te werken met de andere mensen bij Shell, omdat dit over het algemeen hele leuke mensen zijn. Verder bevalt mij het internationale karakter van het bedrijf me heel goed. Ik reis zelf niet heel vaak naar werk op locatie of vergaderingen in het buitenland, maar je hebt wel heel vaak contact met de mensen die daar aanwezig zijn. Verder vind ik het mooi om te merken dat er veel gebeurt in zo'n internationaal bedrijf. Er gaan gigantische bedragen in om, en je levert eigenlijk direct een bijdrage aan de wereld. Daar bovenop is de werkcultuur heel gebaseerd op het feit hoeveel je gedaan krijgt, en je niet enkel wordt afgerekend op het aantal uren dat je werkt.

Waar zie je jezelf in de toekomst?

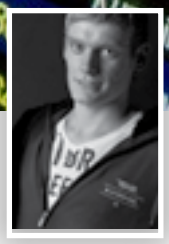
Toevallig krijg ik na mijn verlof al weer een nieuwe baan. Ik ga dan voor een periode van twee jaar meelopen met de CIO van Shell Technical and Competitive IT. Ook daarna wil ik bij Shell blijven werken, omdat ik hier nog heel veel mogelijkheden heb om mezelf te ontwikkelen. De afgelopen zeven jaar heb ik al verschillende dingen gedaan, en dat wil ik ook in de toekomst blijven doen.

Dankjewel voor het interview!

//Artikel

Narrowcasting: Schermen overal

Altijd en overal informatie



Door: Michel Brinkhuis
Redacteur I/O Vivat

Je kunt tegenwoordig niet meer een winkel binnenlopen of de aanbiedingen flitsen voorbij. Bijna elke ondernemer heeft wel een aantal beeldschermen in zijn zaak hangen. Ook als je op het station bent zie je overal animaties op grote schermen voorbij komen. Dit concept heet narrowcasting. Pakken we de Wikipedia-definitie erbij, dan lezen we: "Narrowcasting is het door middel van audiovisuele displays benaderen van een of meer specifieke doelgroepen, op een specifieke plaats en op specifieke momenten. De bedoeling is dat de content zoveel mogelijk op maat is gesneden voor de ontvanger." Het is dus eigenlijk het tegenovergestelde van televisie kijken. Daarbij worden juist beelden getoond die afgestemd zijn op een zo'n breed mogelijk publiek.

Amsterdam centraal

De ontwikkelingen op het gebied van narrowcasting gaan in rap tempo door. Zo hangen er sinds een paar maanden 3D-schermen op station Amsterdam Centraal. Deze schermen zijn ontwikkeld door het bedrijf Dimenco, opgericht door vier mensen die voorheen werkten bij Philips. Zij bieden schermen tot 55 inch aan die autostereoscopisch 3D-beelden kunnen tonen. Deze technologie is inmiddels dusdanig vergevorderd dat de kijkhoek zo groot is dat meerdere mensen 3D-beelden kunnen zien op hetzelfde beeldscherm, zelfs zonder dat er een bril nodig is.

Philips is niet alleen druk bezig met de ontwikkeling van autostereoscopische 3D-schermen voor de 'digital signage markt', die hetzelfde kunnen als de schermen van Dimenco, maar ook werken zij aan dergelijke schermen voor de consumentenmarkt. Dit blijkt uit het feit dat men onlangs op de beurs FPD 2012 in Japan een omgebouwde Macbook Pro met Retina-scherm liet zien, waarop ook 3d-beelden konden worden getoond. Met de ingebouwde webcam werd de positie van de kijker bepaald, en op basis daarvan werden de beelden afgestemd op het linker- en rechteroog.

3D-narrowcasting in winkels

Hoewel je nu in winkels nog geen 3D-schermen ziet waarop reclames te zien zijn, gaat dit vermoedelijk wel de toekomst worden. Uit onderzoek van de Universiteit van Tilburg en Red Bull blijkt dat de tijd dat iemand gemiddeld naar een scherm kijkt met 44 procent toeneemt. Hierbij is een test uitgevoerd die bestond uit drie situaties: een rek Red bull zonder scherm, een rek mét scherm, en een rek met een 3d-scherm. Hierbij keken mensen gemiddeld nog geen twee seconden naar het rek zonder scherm, terwijl bij het rek met een 2D-scherm de aandacht van de consument gedurende 7,6 seconden werd getrokken. De kijktijd bij het 3D-scherm bedroeg gemiddeld bijna elf seconden. Daarnaast bleek ook dat het verkoopcijfer van de energydrank met 8,5 procent steeg.

Figuur 1: 3D-schermen op station Amsterdam Centraal

Smartphones + narrowcasting = winst?

Een nieuwe ontwikkeling die eraan zit te komen is de combinatie van smartphones en narrowcasting. Uit onderzoek van Deloitte bleek dat 68 procent van de consumenten van plan was om voor hun aankopen tijdens de feestdagen eind 2012 hun smartphone te gebruiken. 62 Procent geeft aan hun smartphone te gebruiken om winkellocaties te zoeken, 58 procent om prijzen te vergelijken en de helft van de mensen gaf aan hun smartphone te gebruiken om meer informatie over producten te krijgen tijdens het winkelen.

Het is een trend dat winkeliers klanten proberen te activeren door middel van smartphone specifieke applicaties. Denk aan apps waarmee je korting kunt krijgen als je een speciale kortingsbon uit de app aan de kassa laat zien. En veel winkeliers bieden WiFi aan in hun zaak, waarbij je in de meeste gevallen na het verbinden eerst uitkomt op een speciale 'branded' landingspagina. Uit het onderzoek van Deloitte blijkt ook dat van de mensen in een winkel die een specifieke app van die winkel hebben geïnstalleerd 21% meer aankopen doen. Een goede binding tussen consument en verkopende partij middels smartphones kan dus van grote waarde zijn.

Als zoveel consumenten toch over een smartphone beschikken, en winkels al vol hangen met beeldschermen, kan er dan geen koppeling tussen die twee nieuwe media plaatsvinden? Het antwoord kan worden gezocht bij NFC-technologie. Hoewel iedereen bij het horen van NFC direct denkt aan een digitale portefuille biedt NFC nog veel meer toepassingen. Door NFC-chips te integreren in prijskaartjes van producten kan een consument z'n telefoon er simpelweg tegenaan houden om meer productinformatie te krijgen. Of door je telefoon te 'tappen' tegen een beeldscherm waarop een actie wordt aangekondigd zou je een extra kortingscode naar je telefoon kunnen sturen.

Mensen kijken 44% langer naar een 3D-scherm

Het bedrijf Park Cast Networks, dat veel van de beeldschermen in parkeergelegenheden in New York en Chigaco verzorgt, denkt ook na over de koppeling van narrowcasting-schermen en smartphones. Op een scherm kan bijvoorbeeld een opdracht worden getoond met een timer ernaast. De opdracht kan bijvoorbeeld zijn: 'Maak een foto van jezelf met een fles Coca Cola in de winkel.' Dat doe je natuurlijk via de app van het bedrijf, en als je de foto instuurt maak je kans op een prijs. Door de timer te tonen, en de actie dus maar een relatief korte tijd te laten lopen, kunnen mensen direct worden geactiveerd in een winkel om iets te doen. En dan is de kans groot dat die persoon ook sneller tot (extra) aankopen over gaat.

Social Media

Het Nederlandse bedrijf Nedap werkt ook aan interactieve beeldschermen voor in winkels. Zij ontwikkelden bijvoorbeeld de Tweet Mirror. Dit grote scherm kan bijvoorbeeld in een modezaak worden gebruikt. Iemand kan er in de kleren die hij/zij wil kopen voor gaan staan, een foto maken en deze direct delen via Twitter of Facebook. Op deze manier krijgt de winkelier eigenlijk een gratis online advertentie, en wel op het twitter-account van degene die zijn potentiële aankopen deelt met al zijn Twitter-volgers.

Coca Cola lanceerde eind 2012 in Zuid Korea ook een campagne, waarvan de videobeelden zich snel verspreidden via social media. In Korea hebben ze diverse Coca Cola-automaten voorzien van Microsofts' Kinect-technologie en een enorm display. Zodra mensen voorbij het scherm lopen verschijnen er bandleden van de boyband 2PM, die in Zuid Korea erg bekend is, die de passanten uitdagen voor een spelletje. Zo kun je bijvoorbeeld worden uitgedaagd om te gaan dansen voor het scherm, en als je dat goed doet dan komt er een gratis flesje Cola uit de automaat. Niet alleen in de winkelcentra waar de automaten staan trekt Coca Cola zo de aandacht, maar omdat het hele concept an sich ook zo uniek is, is een video ervan op Youtube ook al miljoenen keren bekeken.

Narrowcasting ontwikkelt zich in hoog tempo, mede door allerlei technologiën die tegenwoordig vrij eenvoudig en goedkoop te implementeren zijn. Bijna iedereen heeft wel een smartphone, NFC wordt steeds meer ondersteund en Kinect is een vrij goedkope manier om bewegingsinteractie te kunnen implementeren. En mocht je winkelen om het winkelen niet zo leuk vinden, dan wordt het dankzij al die mooie technologieën die op steeds meer plaatsen opduiken tóch nog leuk.

Figuur 2: Jongeren worden geactiveerd door een Coca Cola-automaat

Bronnen

Dimenco: http://bit.ly/ZrILY5
3DTVMagazine: http://bit.ly/SE7RQX
Philips: http://bit.ly/WHi8u5
RedBull onderzoek: http://bit.ly/TDSI8L
DigitalSignageToday: http://bit.ly/UWUD4x
Nedap Retail: http://bit.ly/TDSqt5
Madison Blog: http://bit.ly/W37v7c

TREsPASS

Informatie beter beveiligen met scenario's

Door: Wolter Pieters
Vakgroep DIES

Iedere organisatie beschikt over informatie die beter niet in de buitenwereld terecht kan komen. Of het nu gaat om geheime ingrediënten, beursgevoelige gegevens of klantendatabases, er is altijd wel iets te beschermen. Tegelijk zijn de mogelijkheden waarop deze informatie toch de organisatie kan verlaten eindeloos. Ze wordt geoutsourcet naar een cloud provider, door een medewerker mee naar huis genomen, of met laptop en al gestolen. Hoe complexer de informatie-infrastructuur, hoe moeilijker dit te doorgronden is. Daar komt nog bij dat mensen een belangrijke rol spelen in de beveiliging: laat je iemand binnen die eruit ziet als een loodgieter en zegt dat er een afspraak is gemaakt, of geef je je wachtwoord als iemand belt die zegt systeembeheerder te zijn? Iemand die geïnteresseerd is in de gevoelige informatie heeft vele mogelijkheden om binnen te komen.

Penetration testing

Om te kijken welke aanvalsscenario's het hoogste risico met zich meebrengen kun je penetration tests laten uitvoeren. Een gespecialiseerd bedrijf probeert dan binnen te dringen bij je organisatie. In het simpelste scenario wordt dit op afstand via het internet gedaan. Maar er kan ook fysieke toegang aan te pas komen, en zelfs social engineering, het manipuleren van mensen. In het laatste geval moet je goede procedures hebben om te zorgen dat mensen niet onnodig belast worden. Wij hebben dit eerder laten zien in een experiment. Daarbij werd aan medewerkers van de UT een laptop ter beschikking gesteld om te evalueren, en studenten probeerden deze laptops voor ons terug te stelen. Vele geslaagde pogingen laten zien dat niet iedereen even goed oplet, maar veel pogingen mislukten ook juist doordat iemand wèl ingreep. Met penetration testing kun je dus bepalen welke scenario's in de praktijk het vaakst slagen, en daarmee het eerst in aanmerking komen voor maatregelen. Maar hoe kom je aan de scenario's?

Attack trees

In de beveiligingswereld worden vaak zogeheten "attack trees" gebruikt om aan te geven op welke manieren een aanvaller een bepaald doel kan bereiken. Voor het hoofddoel, het verkrijgen van toegang tot een stuk informatie, moet hij dan subdoelen halen. Zo kan hij bijvoorbeeld een laptop stelen waarop de informatie staat, of hij kan een wachtwoord achterhalen en op afstand inloggen. Om een laptop te stelen moet hij toegang verkrijgen tot de laptop, en hij moet de laptop mee naar buiten krijgen zonder ontdekt te worden. Zo wordt de boom van mogelijkheden steeds groter. Het blijft echter mensenwerk om de attack trees op te stellen. Daardoor worden vaak mogelijkheden over het hoofd gezien.

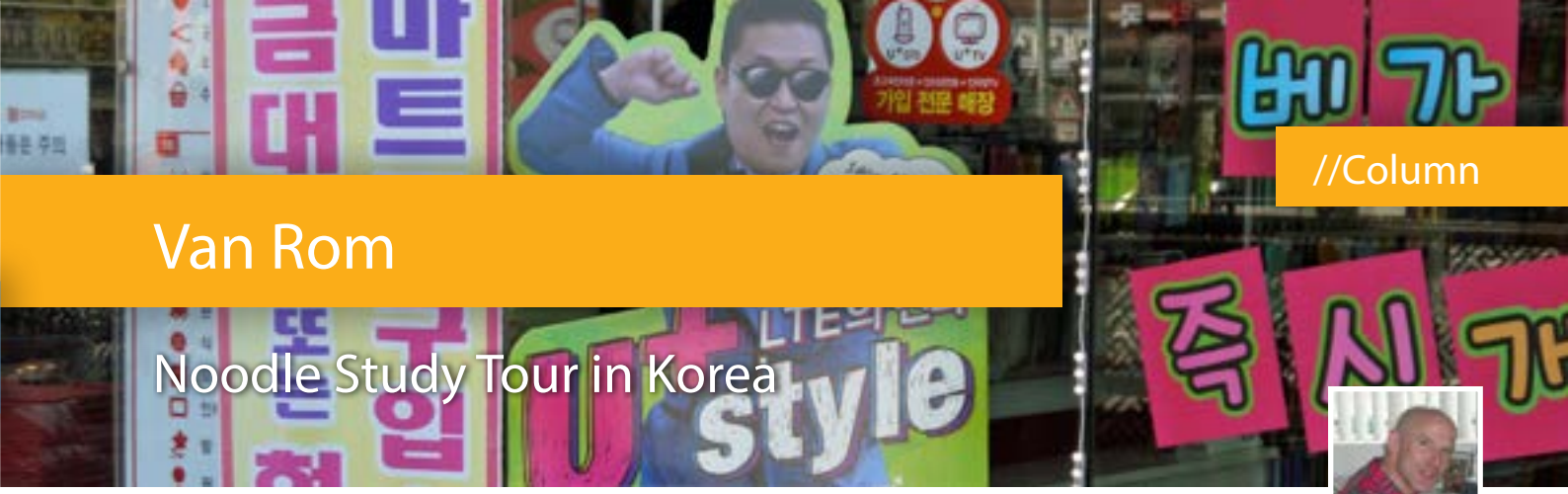
Attack navigators

In ons eerdere project VISPER hebben we "attack navigators" ontwikkeld die scenario's automatisch genereren uit een model van de organisatie. Hierbij worden ruimtes, mensen, computers, en gegevens gerepresenteerd in een graaf, en bepalen policy's welke acties er mogelijk zijn. Op die manier kun je doorrekenen op welke manieren een aanvaller van buiten de organisatie (of van binnen de organisatie!) bij zijn doel kan komen. In het Europese project TREsPASS ontwikkelen we deze navigators verder, zodat we ook kwantitatieve eigenschappen zoals de moeilijkheid van een aanval kunnen meenemen. In dit project werken we samen met 16 andere partners uit heel Europa, en het totale budget bedraagt maar liefst 13,5 miljoen euro. Uiteindelijk kunnen organisaties met de ontwikkelde tools vaststellen welke scenario's het meeste risico met zich meebrengen, en hoe effectief beveiligingsmaatregelen waarschijnlijk zullen zijn.

Meer info:

www.trespass-project.eu

www.utwente.nl/ewi/visper/



//Column

Van Rom

Noodle Study Tour in Korea

Door: Rom Langerak
Opleidingsdirecteur Informatica

De Noodle Study Tour zit er weer op, en alle deelnemers zijn weer veilig teruggekeerd. Van 23 september tot 20 oktober zijn achtereenvolgens Zuid-Korea en China bezocht (en de meeste deelnemers hebben er daarna nog een paar weken vakantie aan vastgeplakt, in uiteenlopende Aziatische oorden). Ik was eigenlijk van plan de hele periode mee te gaan, maar uiteindelijk duurde de reis in totaal vier weken, en zo lang kan ik de opleidingen natuurlijk niet aan hun lot overlaten. Vandaar dat ik gekozen heb voor de twee weken in Korea, waar ik nog nooit geweest was (en een Chinees hebben we tenslotte allemaal wel eens van binnen gezien).

Het was een geweldige ervaring. Sowieso is een studiereis voor een docentbegeleider een van de meest ontspannen bezigheden die je maar kunt voorstellen, want de studenten organiseren helemaal alles. Ik heb met bewondering gekeken naar de organisatoren, die soms tot diep in de nacht bezig waren om alles te regelen en in te spelen op alle onverwachte dingen die tijdens zo'n reis de kop op steken. Goed gedaan jongens, complimenten!

Het grootste gedeelte van die twee weken waren we in de hoofdstad Seoul (spreek uit: Soh-oel) en dat was een belevenis. Seoul is een miljoenenstad die zo uit een sciencefictionfilm lijkt te komen. Ook als je een uur in de metro hebt gezeten zie je nog steeds wolkenkrabbers. Overal is elektronica, en je ziet maar zelden een Koreaan zonder een smartphone (en dan een maatje groter dan die bij ons) in zijn handen. Zie je een gearmd stelletje, dan hebben ze elk in hun vrije hand een smartphone. En ik zag dames op naaldhakken in de metro, die zonder zich vast te houden toch wisten te balanceren, met twee handen berichtjes intikkend.

Het is onvoorstelbaar hoe de Koreanen erin geslaagd zijn in zo korte tijd zo welvarend te worden. Na de Koreaanse oorlog (1950-1953), die aan enkele miljoenen mensen het leven heeft gekost, lag het land volledig in puin en was het een van de armste landen ter wereld. Vervolgens is Zuid-Korea onder enkele (overigens behoorlijk rauwe) militaire dictaturen weer helemaal economisch opgebloeid, en de laatste decennia gaat het land steeds meer richting democratie. Als echt Confucianistisch land heeft onderwijs altijd veel aanzien gehad, en Koreaanse ouders betalen zich blauw aan bijlessen voor hun kinderen – die bijlessen kosten zoveel, dat de meeste Koreanen zich maar één kind kunnen veroorloven. Het uiteindelijke doel is natuurlijk je kind op een topuniversiteit zien te krijgen. Koreaanse universiteiten kennen trouwens geen zak/slaagregeling. Een examen doe je maar één keer, herkansingen zijn er niet. En haal je een onvoldoende, geen probleem, die komt gewoon op je cijferlijst, je diploma krijg je toch wel, en jij mag bij je sollicitatie zelf uitleggen hoe het komt dat daar een onvoldoende staat…. Dat wil natuurlijk niemand, en omdat je een slecht cijfer nooit meer weggepoetst krijgt, werken de studenten keihard. We zagen speciale lokalen waar studenten tussen de bedrijven door konden slapen, omdat ze soms dagen van wel 20 uur maken!

Overigens maken Koreanen een hele vriendelijke en ontspannen indruk. En ze gedragen zich voorbeeldig in het openbaar. Is iemand dronken, dan waggelt ie een beetje, maar veel meer last heb je er niet van. Ik heb slechts één keer een incident gezien: een dronken man maakte zich in de metro zo kwaad over het feit dat een medereiziger een bejaardenstoel bezet hield, dat ie uiteindelijk door de politie verwijderd moest worden. Die medereiziger op de bejaardenstoel was overigens wel één van onze studenten....

Sinds april 1992 is dr. ir. Rom Langerak universitair docent bij de Formal Methods and Tools groep van de faculteit EWI. Romanus (Rom) werd op 1 februari geboren in Dordrecht en ging naar het Christelijk Lyceum aldaar. Hij haalde op de Universiteit Twente met lof zijn studie Toegepaste Wiskunde, waar hij afstudeerde op een onderwerp over Databases. Het is dan ook niet vreemd dat hij na zijn afstuderen ging promoveren bij de toenmalige faculteit Informatica. Na zijn promoveren in 1992 bleef hij bij de faculteit werkzaam.

Rom houdt van literatuur, filosofie, gitaar spelen, biljarten en Taekwondo. Sinds september 2009 is hij de opleidingsdirecteur Informatica, een taak die hij met liefde zal gaan uitvoeren om zo het onderwijs voor zowel studenten als docenten

Anatomie van een Pentest

Kijken door de ogen van een hacker

Door: Herman Slatman
Redacteur I/O Vivat

Beveiliging van gegevens en informatiesystemen is tegenwoordig vrijwel onontbeerlijk geworden. Bijna dagelijks verschijnen er in de media berichten waarin gesproken wordt over het lekken van privacygevoelige gegevens zoals wachtwoorden en creditcardgegevens. Beveiligingsonderzoekers en andere mensen die werkzaam zijn in de informatiebeveiligingsbranche hebben de laatste jaren uiteraard niet stil gezeten om dit aantal te doen afnemen, en dit hebben zij met name door betere beveiligingsmechanismen te implementeren gerealiseerd. Black-hat hackers zitten echter ook niet stil: zij maken gebruik van de nieuwste tools, ontwikkelen nieuwe methoden en nemen direct kennis van de laatste zero-day attacks. De wereld van de informatiebeveiliging lijkt zo een eeuwigdurend kat-en-muisspel te zijn.

Iemand die als het ware op het grensvlak tussen bovengenoemde partijen opereert is de pentester, die wordt ook wel ethisch hacker genoemd. Een pentester kan in opdracht van een instantie een systeem of netwerk van die instantie onderzoeken op de veiligheid daarvan tijdens een zogenaamde pentest. Hij maakt hierbij onder andere gebruik van dezelfde tools die kwaadwillenden gebruiken om in te breken op het systeem of netwerk en om deze te exploiteren. In dit artikel zal ik schrijven over wat een pentest inhoudt en hoe deze in grote lijnen in elkaar steekt. Daarbij zullen ook de 'tools of the trade' aan bod komen.

DISCLAIMER

Het uitvoeren van een pentest op een bepaalde instantie is in de meeste gevallen illegaal als hier niet expliciet toestemming voor gegeven is door desbetreffende instantie.
I/O Vivat is in geen enkel geval aansprakelijk voor eventuele schade die gerelateerd kan worden aan dit artikel.

Wat is een pentest?

Een pentest is, zoals hiervoor al kort werd beschreven, een test die uitgevoerd wordt op een systeem of netwerk om onderzoek te doen naar de veiligheid van het desbetreffende systeem of netwerk. De test wordt uitgevoerd door een pentester, of een groep van pentesters en dit gebeurt in opdracht van de instantie die eigenaar is van het te testen systeem of netwerk.

Het grote verschil tussen een pentest en het daadwerkelijk misbruiken van een systeem zit hem in het feit dat er bij een pentest sprake is van autorisatie. De pentester heeft een contract opgesteld met de instantie waarin staat dat hij gerechtvaardigd is om zwakheden in het systeem te gebruiken om binnen te dringen op het systeem. Zo kan hij mogelijke zwakheden in de beveiliging ontdekken.

Een ander punt waarop een pentest afwijkt van een inbraak is dat de motivatie van de pentester anders is dan die van een black-hat hacker. Waar een black-hat mogelijk vooral gemotiveerd is door financieel gewin of het vergaren van bekendheid, is een pentester er op gericht om een instantie te helpen haar beveiliging te verbeteren. Ook zal een ethisch hacker geen gevoelige bedrijfsinformatie doorspelen aan buitenstaanders; black-hats doen dit in bepaalde gevallen wel.

Een pentest kan in de meeste gevallen opgedeeld worden in drie verschillende fases, die hierna besproken zullen worden. Dit artikel is geenszins een compleet naslagwerk voor de perfecte pentest, maar licht slechts een tipje van de sluier.

Fase één: de verkenning

De eerste fase van een pentest bestaat meestal uit het verkennen van het doelwit. Dit is een zeer belangrijke fase, want een pentester krijgt tijdens de verkenning een zeer grote hoeveelheid gegevens over zijn doelwit tot zijn beschikking. Een groot deel van deze informatie zal een pentester nodig hebben tijdens de tweede fase.

Als pentester probeer je te denken als een black-hat hacker. Dit houdt dan ook voornamelijk in dat hij een pentest uitvoert zoals een black-hat zou inbreken op een systeem. Een eerste stap is om een passieve verkenning uit te voeren. Hierbij wordt voornamelijk gebruik gemaakt van informatie over het doelwit die publiek toegankelijk is. Er wordt zo geen enkele interactie met het doelwit zelf gepleegd, buiten het doorzoeken van de website van het doelwit, waardoor deze redelijkerwijs niet door heeft dat er een onderzoek naar de bedrijfssystemen plaatsvindt.

De website van het doelwit vormt een belangrijke bron van informatie. Zo kunnen bijvoorbeeld interessante gegevens als fysieke adresgegevens, telefoonnummers, emailadressen, openingstijden en werknemersgegevens gevonden worden. Vooral de secties op de website die nieuws, aankondigingen en vacatures bevatten, leveren vaak veel bruikbare informatie op, omdat deze secties aangeven waar een doelwit mee bezig is. Zo kunnen er bijvoorbeeld aankondigingen zijn over nieuwe systemen die in gebruik genomen zijn, of is er een vacature beschikbaar voor 'beveiligingsspecialist' die verstand heeft van SCADA-netwerken.

Het gebruik van Google Directives kan ook een zeer goede bron van informatie zijn. Met behulp van Directives kunnen extra parameters meegegeven worden aan een zoekopdracht, waardoor het aantal zoekresultaten meestal beperkt wordt, maar deze wel zeer gerichte resultaten oplevert. Zo kunnen bijvoorbeeld alle documenten die op een website aanwezig zijn, gevonden worden. In combinatie met de tool 'MetaGooFil', die metadata van documenten van over het hele internet verzamelt, vormt dit een unieke kijk op het doelwit, omdat zaken als gebruikers- en systeemnamen vaak aan het licht komen.

Naast alle digitale wegen om informatie te vergaren kan een pentester uiteraard ook gebruikmaken van social engineering om aan gegevens te komen. In combinatie met eerder vergaarde informatie, zoals de naam van een werknemer technische dienst en door het manipuleren van een baliemedewerk(st)er, zou een pentester fysieke toegang kunnen krijgen tot ruimtes die normaal gesproken onbereikbaar zouden moeten zijn voor buitenstaanders. Daar kan hij op zoek naar papieren data, of een keylogger of backdoor installeren op een computersysteem om meer bruikbare digitale data te vergaren.

Aan het eind van de verkenningsfase heeft een pentester in de meeste gevallen een ongelooflijke hoeveelheid informatie. Het is dan zaak om deze informatie netjes te ordenen bijvoorbeeld door het samenstellen van lijsten met IP-adressen, mailadressen en URLs. In overleg met de opdrachtgever wordt vastgesteld of de scope van de pentest eventueel aangepast moet worden, of dat er bepaalde IP-adressen uitgesloten moeten worden van de pentest.

Fase twee: de ontdekking

Tijdens de verkenningsfase zijn verschillende hostnamen en URLs gelinkt aan IP-adressen. In de ontdekkingsfase worden deze IP-adressen gerelateerd aan open poorten en draaiende services. Een optimale beveiliging zou inhouden dat een systeem helemaal afgesloten is: geen enkele poort staat open en er zijn dus geen services om mee te communiceren. In de realiteit is dit echter geen optie: een webserver waarop poort 80 afgesloten is, heeft geen nut. Elke open poort, draaiende service of connectie naar een ander netwerk kan een ingang vormen voor een pentester.

De eerste stap is het vaststellen of een systeem 'live' is. Dit gebeurt door middel van het zenden van pings naar een bepaald IP. Het systeem kan een antwoord geven op de ping door een Echo Reply pakket te sturen. De tool FPing kan gebruikt worden om zogenaamde ping sweeps uit te voeren: Het pingen van een groot aantal opvolgende IP-adressen. De informatie die een pentester krijgt van een ping of ping sweep dient niet als uitgangspunt gebruikt te worden in de rest van de fase. Een ICMP Echo Request pakket wordt namelijk niet altijd beantwoord, zoals het geval is als deze pakketten door een firewall uit het netwerkverkeer gefilterd worden.

Na het pingen van systemen heeft een pentester een idee van de actieve servers. Hij kan dan verder gaan met het scannen van open poorten op deze systemen. Hierbij zullen echter ook de machines die inactief leken meegenomen worden, om geen enkele mogelijke ingang uit te sluiten. Bij het scannen van open poorten kijkt een pentester uiteraard naar welke services er op een systeem draaien. Hierbij is NMap, of een vergelijkbare tool, onmisbaar. NMap stelt een pentester in staat om enkele

> "De website van het doelwit vormt een belangrijke bron van informatie"

Figuur 1: Trinity gebruikt NMap in The Matrix Reloaded om een kwetsbare server te vinden.

verschillende soorten poortscans uit te voeren, zoals een TCP Connect, SYN, UDP of Xmas scan. De verschillende soorten scans kunnen in bepaalde situaties verschillende resultaten opleveren, waardoor kennis van alle soorten scans zeker aan te raden is. NMap wordt niet enkel gebruikt voor het zoeken van de open poorten, maar kan ook gebruikt worden om vast te stellen welke versies van services er draaien en welk besturingssysteem er draait.

> "Hierbij is NMap, of een vergelijkbare tool, onmisbaar"

Soms kan een pentester zich, met enkel de kennis van de draaiende services, toegang verschaffen tot een systeem. Standaardgebruikersnamen en –wachtwoorden werken lang niet altijd, maar ze zijn zeker het proberen waard. Als dit niet lukt gaat een pentester op zoek naar kwetsbaarheden in het systeem. Kennis van de verschillende services en de verschillende versies daarvan is belangrijk. Zwakheden in een service kunnen in een nieuwe versie van de software gepatcht zijn, maar als deze nieuwe versie niet draait heeft een pentester wellicht al een toegangsweg gevonden. Een tool die in deze fase veel gebruikt wordt is Nessus. Dit is een programma dat scant op verschillende zwaktes op een systeem. Met de informatie van deze scan kan een pentester een lijst van kwetsbaarheden opstellen die mogelijk te misbruiken zijn om toegang tot het systeem te krijgen.

Fase drie: de exploitatie

Het uitvoeren van een exploit, om uiteindelijk administratieve toegang te verkrijgen (en te behouden) tot een systeem kan gezien worden als het einddoel van een pentest. Zodra het de pentester gelukt is zich toegang te verschaffen, kan hij een verslag schrijven over hoe de status van de beveiliging van een systeem en hierbij aanbevelingen voor verbeteringen geven. Wat er voorafgaat aan dit verslag is wellicht een stuk interessanter voor de lezer. Wat er precies plaatsvindt in deze fase ligt niet direct vast omdat in feite elk systeem anders is. Zelden zal een pentester precies dezelfde configuraties tegenkomen bij verschillende doelwitten en zal hij dus ook telkens andere wegen moeten bewandelen om binnen te raken.

Een eerste stap is het verkrijgen van een toegang door proberen in te loggen op enkele van de gevonden services. Hierbij kan gebruik gemaakt worden van Medusa en Hydra bijvoorbeeld. Dit zijn beide tools die op brute-force wijze kunnen proberen in te loggen op een bepaalde service. Lijsten met gebruikersnamen en wachtwoorden kunnen als command line argumenten meegegeven worden om deze door de tools te laten proberen op het doelwit. Hierbij kan onder andere gebruik gemaakt worden van gebruikersnamen die tijdens de verkenningsfase aan het licht kwamen. Sommige hackers bouwen een dictionary van verschillende wachtwoorden die enkele gigabytes kan beslaan. Het onderhouden van zo'n lijst kost veel tijd, maar het is een beproefd middel waarmee nog vaak toegang verschaft kan worden tot systemen.

Dit artikel zou niet compleet zijn zonder

Figuur 2: BackTrack is een Linux-distributie die een uitgebreid arsenaal aan pentesting gereedschappen levert.

Metasploit besproken te hebben. Metasploit is een open-source framework dat gebruikt kan worden om exploits op systemen uit te voeren. Daarnaast kunnen exploits ontwikkeld en gedeeld worden met andere beveiligingsonderzoekers en hackers. Een slimme hacker gebruikt Metasploit op secure wijze: kies een doelwit, zoek er een passende exploit bij en stel de gewenste payload vast. Het is af te raden om als een krankzinnige met exploits te gaan strooien op een willekeurig doelwit. Daarom is het verstandig om de keuze voor een exploit te baseren op de Nessus scan uit de ontdekkingsfase.

Zoals beschreven kan Metasploit gebruikt worden voor het uitvoeren van exploits. Met de juiste kennis kan een doelwit binnen enkele tellen volledig gecompromitteerd zijn. Een aanval met Metasploit verloopt in grote lijnen volgens de volgende stappen:

- msf > search: zoekt een patch die mist volgens Nessus

- msf > use: stelt een exploit in

- msf > show payloads: geeft alle mogelijke payloads weer

- msf > set payload: stelt een payload in

- msf > show options: geeft de opties voor de payload weer

- msf > set option: stelt de optie in

Het laatste commando, msf > exploit, start de daadwerkelijke exploitatie van het systeem. Zo kan er bijvoorbeeld een VNC verbinding opgezet worden, of wordt er een shell gestart op het doelwit. Deze is dan volledig overgeleverd aan de hacker.

Wanneer het nauwkeurig uitzoeken van een passende exploit te veel werk is kan er altijd nog gebruik worden gemaakt van de tool Fast-Track. Deze automatiseert het zoeken van open poorten, probeert alle mogelijke exploits op de open poorten en probeert shells te starten. In een zwak beveiligd systeem kunnen er soms op meerdere manieren shells gestart worden. Fast-Track maakt het voor een beginner misschien wel makkelijk, want er hoeft niet veel meer dan een IP-adres als doelwit ingevoerd te worden. De aanval is echter in geen geval 'stil' te noemen. Desalniettemin kan Fast-Track beschouwd worden als een handig hulpmiddel om de veiligheid van de eigen systemen aan de kaak te stellen.

> "... is het aan te raden om een pentesting-lab op te zetten"

Zelf aan de slag?

Zoals beschreven is het uitvoeren van een pentest enkel legaal als dit in opdracht van het doelwit gebeurt en de omvang van de test strak is afgebakend met een contract. Mocht je zelf geïnteresseerd zijn in het leren om een pentest uit te voeren, dan is het aan te raden om een zogenaamd pentesting-lab op te zetten. Dit netwerk bestaat mogelijk uit slechts twee machines: een doelwit en een machine vanaf waar de aanval ingezet wordt, maar kan ook bestaan uit meerdere doelwitten. Dit netwerk kan, mocht je niet over voldoende fysieke machines beschikken, ook opgezet worden door gebruik te maken van virtual machines.

Om menselijke fouten, zoals het verkeerd overtikken van een IP-adres, tegen te gaan is het daarnaast van belang om ervoor te zorgen dat het netwerk helemaal los staat van het Internet. Zo kan er geen dataverkeer plaatsvinden met de buitenwereld en zal je nooit per ongeluk een machine aanvallen buiten je eigen pentesting-lab. Het gebruik van enkel virtuele machines, en het daarbij uitschakelen van de network interface card is hier een goed middel voor.

De verkenningsfase is al met al de makkelijkste fase om als beginnend pentester te oefenen, omdat er weinig kwaad is in het onderzoeken van (mogelijke) doelwitten. De informatie die tijdens deze fase gevonden wordt, bevindt zich immers in het publieke domein. Om het pentesten verder onder de knie te krijgen is aan te raden om niet te moeilijk te beginnen. Rust een machine uit met bijvoorbeeld Windows XP (zonder Service Packs). In deze versie van Windows zijn er nog een behoorlijk aantal lekken aanwezig die met Metasploit geëxploiteerd kunnen worden. Installeer op zo'n machine ook enkele services, zoals een mailserver, FTP of een webserver en maak hiervoor verschillende gebruikers aan. Probeer met de technieken uit de ontdekkingsfase informatie over deze services te weten te komen, en daarnaast, met tools als Hydra of Medusa om binnen te raken bij de service. De lat kan je voor jezelf steeds hoger leggen, bijvoorbeeld door Service Packs te installeren voor Windows XP, of om een ander besturingssysteem proberen te compromitteren.

Conclusie

De laatste tijd zijn er veel berichten in de media verschenen die een beveilingslek bij een instantie aan het licht brachten. Bedrijven kunnen een pentest uit laten voeren door een ethisch hacker, of pentester, die voor hen onderzoekt of de beveiliging van hun systemen van voldoende niveau is, en hen kan adviseren als dat nodig is. Een goede pentest bestaat uit drie verschillende fasen: de verkennings-, ontdekkings- en exploitatiefase. Tijdens elke fase worden andere tools gebruikt om het doel van de fase te bereiken. Één van de belangrijkste aspecten van een pentest blijft echter toch dat een pentester tijdens een test legaal door de ogen van een hacker kijkt.

Bronnen

Penetration Testing - Procedures and Methodology
(ISBN 978-1-4354-8367-5)
EC-Council

The Basics of Hacking and Penetration Testing - Ethical Hacking and Penetration Testing Made Easy
(ISBN 978-1-59749-655-1)
Patrick Engebretson

http://www.backtrack-linux.org/

Turing-award winnaar in beeld

Andrew Chi-Chih Yao, fundamentele bijdragen aan theory of computation

Door: Niek Tax
Redacteur I/O Vivat

Het zal weinig Inter-*Actief*-ers ontgaan zijn dat studiereis Noodle afgelopen september is vertrokken naar Zuid-Korea en China. Naast vele andere universiteiten en bedrijven in deze landen is tijdens deze reis ook de prestigieuze Tsinghua University in Beijing bezocht, waar sinds 2004 in de naam van Andrew Chi-Chih Yao een heuse Turing-award winnaar zijn onderzoek doet.

Andrew Chi-Chih Yao

Op 24 december 1946 werd Andrew Yao geboren in Shanghai. Kort na Andrews geboorte verhuisde zijn ouders naar Hong Kong om enkele jaren later te emigreren naar Taiwan, waar Andrew grotendeels opgroeide. Op 21-jarige leeftijd behaalt Andrew een bachelorgraad in de Natuurkunde aan de National University of Taiwan, waarna hij naar Harvard vertrekt om daar zijn natuurkundemaster en Ph.D te behalen onder begeleiding van Nobelprijswinnaar Sheldon Glashow. Na een start in de natuurkunde maakt Yao het verstandige besluit zich met informatica te gaan bezighouden - in slechts twee jaar tijd behaald Yao zijn Ph.D in de informatica op het onderwerp computational complexity. In de vijf jaar die hierop volgen zal Yao als onderzoeker aan de wiskunde afdeling van MIT en aan de computer science afdeling van Stanford fundamentele bijdragen leveren aan de wetenschap van algoritmiek. Yao's bekendste bijdrage aan de computational complexity is Yao's principle, waarin Yao het verband aantoont tussen de complexiteit van gerandomiseerde algoritmes en de complexiteit van deterministische algoritmes. Naast bijdragen in de algoritmiek heeft Yao ook significante bijdragen geleverd aan de cryptografie. In de komende paragrafen zullen elk een van Yao's voornaamste bijdragen worden uitgelicht.

Yao's principle

Kort gezegd zegt Yao's principle dat wanneer men de ondergrens van de kosten van een gerandomiseerd algoritme wil berekenen, het voldoende is om de complexiteit van een deterministische versie van hetzelfde algoritme te beschouwen waarbij de invoer getrokken is uit een kansverdeling. Waar bij een deterministisch algoritme sprake kan zijn van worst-case invoer: een invoer die de worst-case situatie tot resultaat heeft, kan men bij een gerandomiseerd algoritme slechts spreken van een worst-case invoerverdeling. De verwachtingswaarde van de tijdscomplexiteit van een gerandomiseerd algoritme met worst-case invoer gelijk is aan de gemiddelde tijdscomplexiteit voor het equivalente deterministisch algoritme voor de worst-case verdeelde invoer. Yao bewees deze stelling aan de hand van de in de speltheorie bekende minimax-stelling, die ook in het vakgebied van artificial intelligence veel-

Figuur 1: Andrew Chi-Chin Yao geeft zijn computer science college.

vuldig wordt gebruikt. Yao's principle is uitgegroeid tot een van de fundamentele technieken om gerandomiseerde algoritmen en hun complexiteit te beschouwen.

Yao's test

In 1982 stelde Yao een test op voor het identificeren van pseudo-random reeksen tussen compleet random reeksen. Yao stelt dat een woordenreeks slaagt voor Yao's test wanneer een machine met redelijke rekenkracht de woordenreeks niet kan onderscheiden van een willekeurig uniform gegenereerde reeks. Yao's test is hiermee een variant op de binnen cryptografie veel gebruikte next-bit test, waarbij het al dan niet kunnen voorspellen van het (i + 1)ste teken na i gegeven voorgaande tekens door een machine met redelijke rekenkracht wordt gebruikt voor het onderscheiden van pseudo-random reeksen.

Yao's Miljonairsprobleem

Yao's Miljonairsproblem is een probleem waarbij twee miljonairs, Alice en Bob, beide graag willen weten wie van hen beide rijker is zonder daarbij de hoeveelheid geld wat ze zelf in bezit hebben aan de ander te vertellen. Yao's Milljonairsprobleem is analoog aan een generieker probleem waarbij men de probeert te achterhalen van twee getallen a en b of getal a groter of gelijk is aan b, waarbij de waarden van a en b niet bekend gemaakt mogen worden. Binnen de e-commerce is dit een relevant probleem, aangezien dergelijke applicaties soms cijfers moeten vergelijken waarvan het belangrijk is dat deze vertrouwelijk blijven. Andrew Yao was zelf de eerste die een algoritme publiceerde die Yao's Miljonairsprobleem oploste. Inmiddels zijn vele algoritmen gepubliceerd die Yao's Miljonairsprobleem oplossen, waaronder oplossingen die efficiënter zijn dan Yao's oplossing die zowel in tijdscomplexiteit als geheugencomplexiteit exponentieel is.

Dolev-Yao model

Het Dolev-Yao model is een formeel model wat gebruikt kan worden om eigenschappen van interactieve protocollen te bewijzen, vaak beveiligingsprotocollen. Binnen het Dolev-Yao model wordt een netwerk gerepresenteerd door een set abstracte machines die berichten kunnen uitwisselen, waarbij deze berichten bestaan uit formele termen. Onderdeel van een netwerk in het Dolev-Yao model is een "tegenstander" die in staat is elk bericht dat in het netwerk wordt verstuurd te onderscheppen en te creëren en versturen. Security-protocollen worden slechts veilig geacht wanneer binnen een netwerk met een dergelijke "tegenstander". Binnen het security vakgebied wordt dit model veelvuldig gebruikt om veiligheidseigenschappen zoals vertrouwelijkheid en integriteit binnen een communicatieprotocol formeel te bewijzen.

> "Andrew Yao was zelf de eerste die een algoritme publiceerde die Yao's Miljonairsprobleem oploste"

Figuur 2: Logo van de universiteit van Tsignhua.

Tsinghua Universiteit

De Tsinghua universiteit is de universiteit waar Andrew Chih-Chih Yao tegenwoordig zijn onderzoek doet en tevens een van de universiteiten die door studiereis Noodle zijn bezocht. Tsinghua is gevestigd aan de rand van Beijing en behoord wereldwijd tot de betere universiteiten. De QS World University Rankings plaatst Tsinghua in de jaarlijkse meting van 2012 wereldwijd op een de 48e plaats overall en zelfs op een 11e plaats binnen de Engineering & Technology richting (waaronder informatica). Bezoekers van de Noodle-studiereis kunnen onderschrijven dat de universiteit inderdaad aandeed als een excellente universiteit.

Bronnen:

Andrew Chi-Chih Yao (2000)
http://amturing.acm.org/award_winners/yao_1611524.cfm

ANDREW CHI-CHIH YAO (2005)
http://www.cs.princeton.edu/~yao/myvita.pdf

Institute for Theoretical Computer Science (2011)
http://itcs.tsinghua.edu.cn/yao

1996 Knuth Prize - Andrew C.-C. Yao
http://www.sigact.org/Prizes/Knuth/1996.html

Tsinghua University (2012)
http://www.topuniversities.com/institution/tsinghua-university

Cybersecurity

Wat doet Nederland om haar digitale landsgrenzen te verdedigen?

Door: Stijn van Winsen
Redacteur I/O Vivat

In het dagelijks leven wordt ICT steeds bepalender. Een samenleving zonder ICT en internet is al nauwelijks meer denkbaar en de nood om deze essentiële voorzieningen te verdedigen wordt hoger. In Iran is in 2010 een worm gevonden gemaakt om een kernprogramma te ontregelen. Een complex stuk software die een groot deel van Iran had kunnen ontregelen. Het antwoord op de vraag of het belangrijk wordt voor een land om zichzelf te verdedigen is dus een makkelijke. Maar hoe moet een land zichzelf verdedigen?

Cyberwar en cyberterrorism

De droom van iedere hollywoodwriter en nerd; een oorlog volledig gevoerd op de digitale snelweg. Met flitsende lampjes en voorbijkomende eentjes en nulletjes het land verdedigen tegen de kwade vijand. Maar hoe reëel is deze dreiging überhaupt? In een advies van de 'Adviesraad Internationale Vraagstukken' (AIV) en de 'Commissie van Advies inzake Volkenrechtelijke Vraagstukken' (CAVV) wordt gesteld dat cyberwar en cyberterreur op zich geen reëel dreigingen zijn. Zij stellen dat de kans op een volledige digitale oorlog zeer klein is, en dat als er een cyberwar gevoerd gaat worden door een staat, dit alleen maar zal gebeuren in combinatie met reguliere oorlogsdaden. In oorlogstijd is het makkelijker om met een gerichte bom infrastructuur plat te leggen dan met een voor datzelfde doel geschreven malware.

Dit neemt niet weg dat er aandacht moet worden besteed aan defensie op digitaal gebied. The Lipman Report, een rapport van het amerikaanse beveiligingsbedrijf Guardsmark, stelt dat vele belangrijke sectoren van westerse landen momenteel een erg groot risico lijden op gebieden als educatie en publieke voorzieningen. Hierdoor is ook de financiele sector in gevaar en dat door het toenemend gevaar op cybergebied en de slechte verdediging van landen die er nu is. Een cyberwar komt er dus niet snel, maar verdedigen moeten we ons zeker. Vooral de kennis van inlichtingendiensten dient vergroot te worden en er moet ingezet worden om online spionage tegen te gaan.

Oprichting

Vandaar dat het Pentagon in mei 2010 het nieuwe USCYBERCOM (U.S Cyber Command) heeft opgericht om Amerikaanse militaire netwerken te verdedigen en de systemen van andere landen aan te kunnen vallen. Ook de Europese Unie heeft aangegeven het ENISA (European Network and Information Security Agency) uit te willen breiden om beter met deze nieuwe dreiging om te kunnen gaan.

In Nederland heeft de overheid in 2011 besloten een Taskforce Cyber te starten onder leiding van Kolonel Hans Folmer, die deel uit maakt van de landmacht. In eerste instantie krijgt het commando vooral een defensieve taak, maar gaat het ook de mogelijkheden tot het maken van digitale wapens onderzoeken. Net zoals het Pentagon en de EU beseft de Nederlandse overheid dat ze iets moet doen.

Nationale Cyber Security Strategie

In juli 2011 kwam het ministerie van Veiligheid en Justitie met het zogenoemde Nationale Cyber Security Strategie (NCSS). Hierin zijn het doel en de actielijnen van cyber security verwerkt waarop Nederland zich gaat richten. Onderdeel hiervan is het inrichten van een Cyber Security Raad en het Nationaal Cyber Security Centrum (NCSC). Omdat al deze kennis voor het verdedigen van het land op Cyber gebied niet bij één partij kan liggen wenst het kabinet ook veel samenwerking van deze centra met het bedrijfsleven. Private en publieke partijen moeten bij het NCSC samen komen om hun expertise en kennis te delen en te helpen bij eventuele dreigingen en incidenten. Meer over het Nationale Cyber Security Strategie is te vinden bij de bronvermelding.

Nationaal Cyber Security Centrum

Als onderdeel van het NCSS is sinds 1 januari 2012 kolonel Hans Folmer bezig met het inrichten van het Nationaal Cyber Security Centrum. Doel van dit centrum is het gezamenlijk vergroten van de weerbaarheid van de Nederlands samenleving in het digitale domein. Hiervoor doet zij verschillende dingen, zoals

het creëren van een gezamenlijk en integraal beeld van de actuele dreigingen van ICT. Ook moet het centrum een platform zijn voor het uitwisselen van kennis, expertise en informatie tussen bedrijven zodat inzicht kan worden verkregen in ontwikkelingen, dreigingen en trends, en ondersteuning kan worden geboden bij incidentafhandeling en crisisbesluitvorming. Hiertoe werkt zij samen met verschillende securitybedrijven als Fox IT, maar ook met bedrijven zoals het vroegere GOVCERT.NL dat nu opgegaan is in het NCSC.

Internationaal

Op Europees gebied zijn er al 10 landen die deelnemen aan het Cooperative Cyber Defence Centre of Excellence dat gesitueerd is in Tallinn. Het CCDCOE heeft als doel om informatiedeling te bevorderen tussen NAVO landen. Nederland nam voorheen alleen de diensten af, maar stuurt nu zelf ook een officier naar het hoofdkantoor en wordt hiermee de elfde deelnemer. Hierdoor gaat Nederland zich ook bemoeien met de richting die het CCDCOE de komende jaren gaat voeren en is zij nauwer betrokken bij de kennisuitwisseling tussen deze landen.

Ook andere landen zijn bezig met het opzetten van centra om te onderzoeken hoe ze zichzelf moeten verdedigen en andere landen moeten aanvallen. Landen als Amerika en China geven hier all veel geld aan uit en veel andere landen als Duitsland en Engeland volgen nauw. Nederland ligt niet voorop, maar is wel verder dan de meeste andere landen.

Conclusie

Er gebeurt steeds meer op digitaal gebied en veel landen zien in dat het steeds belangrijker wordt ook de digitale landsgrenzen te verdedigen. Voor Nederland wordt het belangrijk om te investeren in deze nieuwe vorm van Defensie en samen met andere landen kennis uit te wisselen op dit gebied. Hoewel een echte digitale oorlog niet snel zal komen, kan het wel voorkomen dat deze digitale weg gebruikt wordt om informatie te krijgen van de tegenstander en misleidende informatie te plaatsen. Met het nieuwe NCSS zet Nederland in ieder geval een stap in de goede richting.

“Dit neemt niet weg dat er aandacht moet worden besteed aan beveiliging op digitaal gebied”

Nationale Cyber Security Centrum

De Nationale Cyber Security Strategie bevat verschillende hoofdpunten waar Nederland zich op gaat richten op cyber security gebied in de komende 3 jaar. Hierin staat onder andere het oprichten van de Cyber Security Raad en het Nationaal Cyber Security Centrum en het programma voor deze centra voor de komende jaren.

Zo wordt het de taak van het NCSC om dreiging- en risicoanalyses te maken, de weerbaarheid van de vitale digitale infrastructuur van Nederland te vergroten door samen te werken met grote telecombedrijven en daar goede afspraken mee te maken, en de opsporingen en vervolgingen van cybercrime te intensiveren. Ook wil de overheid onderzoek en onderwijs stimuleren door onder andere certificeringen aan te bieden voor informatiebeveiligingsprofessionals. Het NCSS is ook te vinden op http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/

Bronnen:

https://www.ncsc.nl
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking.html

Een reis door Azië

Met Inter-Actief door Zuid-Korea en China

Door: Rick van Galen
Redacteur I/O Vivat

Studiereis Noodle werd georganiseerd vanuit Inter-*Actief* en bracht eind september en in oktober een driewekelijks bezoek aan Zuid-Korea en China. Tijdens het bezoek aan Azië bezochten de Inter-Actievers een aantal bedrijven en universiteiten om te zien wat voor onderzoek men doet in de IT. Het thema was "IT Integrated Lifestyle" – welke technologieën worden er ontwikkeld om het alledaagse leven te verbeteren?

Korea

Bij het bezoek aan Zuid-Korea warden er meteen dingen duidelijk over de rol van technologie in de samenleving. In het openbaar vervoer in Nederland pakt iedereen al snel de smartphone erbij om wat berichten te checken of een spelletje te spelen. In Zuid-Korea wordt dit tot in het extreem uitgewerkt. Bijna iedereen heeft een nieuwe telefoon; het is net alsof telefoons die niet het nieuwste model van Samsung, LG of Apple zijn niet bestaan. Met name de gigantische (5.5 inch scherm) Galaxy Note II was een geliefd object om mee te spelen, te surfen of televisie op te kijken. In het laatste geval kwam er een antenne tevoorschijn die uit de jaren '90 leek te zijn gekomen, op de telefoon geschroefd en uitgeschoven. In Seoul is namelijk overal gratis draadloze televisie te ontvangen, zelfs in de metro.

Buiten de groep westerlingen die zich dagelijks in de metro naar allerlei bestemmingen begaf leek niemand zich te verbazen over de manier waarop Zuid-Koreanen zich overgaven aan hun smartphone. Technologie, en vooral gadgets, zijn onderdeel van de cultuur. In tegenstelling tot de gemiddelde Europeaan is het niet de Koreaan zijn doel om een groot huis te hebben met een grote auto, maar een klein efficiënt huis dat is uitgerust met de nieuwste gadgets, en een kleine stille auto die met elektronica de ervaring voor de rijder het beste maakt. Nieuwbouw bestaat dus vooral uit torenhoge flats waarin elke wooneenheid is uitgerust met (via apps bestuurbare) vloerverwarming, glasvezelverbindingen en bewegingssensoren (die onder andere wc-brilverwarming triggeren). Technologie is er overal en is al onlosmakelijk verbonden met de cultuur.

Ziet men dit ook terug in de bedrijven daar? Dat valt nog wel mee. De bedrijven die we in Daejeon en Seoul bezochten deden niet heel anders aan dan dat je het in Nederland zou verwachten. Innovatie was er zeker: het bedrijf Neo-LAB Convergence werd een pensysteem ontwikkeld dat door middel van kleine (voor de mens onleesbare) codes op bepaalde stukken van het papier geluid af te spelen. Dit kan gebruikt worden in het onderwijs om het leerproces van bijvoorbeeld taal te versnellen. Ook bezochten we 3DOne, dat een technologie ontwikkelt om vlakke LCD-displays zonder brilletjes of andere hulpmiddelen 3D-beelden beter te laten weergeven. Hoewel de 3D-weergave veel natuurlijk was dan de 3D-technologie die nu in Nederland te koop is, moet wel gezegd worden dat dit effect alleen

Figuur 1: Onderweg naar een bedrijf in Seoul

zo goed werkt als je precies op de goede plek voor het scherm gaat zitten.

De universiteiten in Zuid-Korea doen erg ambitieus aan. Dat is niet raar; de cultuur in Korea is enorm gefocust op prestatie en dan vooral het volgen van een goede opleiding. Gevolg is dat 80% van de Koreanen een universitaire opleiding heeft genoten. Weliswaar zijn niet al deze universiteiten van het niveau dat we in Nederland kennen, maar de goede universiteiten in Korea zijn wel *heel* goed. Het Korea Advanced Institute of Science and Technology (KAIST) wordt het "MIT van Azië" genoemd en daar zijn ze erg trots op. Het instituut is een van de beste ingenieursopleidingen in Azië en heeft vooraanstaande projecten op het gebied van robotica. Ook Seoul National University weet haar eigen kwaliteit goed aan te prijzen. De meeste universiteit die we bezochten deden dat, al is het niet duidelijk of deze universiteiten nu ook *echt* betere plekken zijn om onderwijs te volgen of onderzoek te doen als de Universiteit Twente.

China

Het gevoel van een samenleving die rondom technologie draaide verdween in China als sneeuw voor de zon. China is simpelweg een ontwikkelingsland, en een bezoek aan rijke steden kan dat feit niet wegpoetsen. Helemaal niet eigenlijk, als je over de straten rondloopt en oude communistische auto's ziet wegroesten langs de kant van de weg.

Volgens de Nederlandse ambassade in Shanghai is de Chinese IT-industrie een van de meest vooruitstrevende ter wereld. Niet alleen is het, zoals zoveel Chinese zaken, de snelst groeiende IT-industrie ter wereld, maar de gehele Chinese technologiesector probeert af te komen van het imago dat het vooral Westerse producten kan kopiëren voor een lage prijs. De regio rondom Kanton in het zuiden van China zou daarom nu bekend staan als één van de meest innovatieve regio's op het gebied van IT ter wereld – het hoeft alleen Silicon Valley voor zich te dulden.

> "De universiteiten in Zuid-Korea doen erg ambitieus aan"

Van deze innovatie ziet men eerlijk gezegd niet zoveel in China. De bedrijven die we bezocht hebben waren niet significant anders dan de Nederlandse startups. Ook aan de bezochte universiteiten viel duidelijk te zien waarom in Nederland men de term 'universiteit' zo wil beschermen; de instituten waar men heel trots op was deden niet anders aan dan een Nederlandse HBO-instelling. De enkele uitzondering hierop was de Tsinghua-universiteit in Beijing die zo mogelijk de beste universiteit van de hele reis was. Niet alleen was deze universiteit de werkgever van enkele (!) Turing-award-winnaars, het streefde ook een programma van excellentie na dat we bij geen enkele ander universiteit kon nastreven. Zie ook het artikel over Andrew Yao in deze Vivat.

Het beste bezoek van de studiereis was aan de Aziatische tak van Microsoft Research in Beijing. Microsoft Research is een verrassend vrije tak – het mag ongericht onderzoek doen naar allerlei zaken zonder dat er een richting aan wordt gegeven door het centrale management. Het gevolg is dat Microsoft Research als 'projectjes' nieuw onderzoek mag doen in zoekmachines en touchscreens die weer leiden tot innovaties in Bing en Windows 8. Zo heeft Microsoft een geavanceerde academische zoekmachine. Microsoft Academic Search is een product waarbij Microsoft door expertise in *entity search* (waarbij gezocht wordt naar objecten waarbij contextinformatie belangrijker is dan wat eruit een PageRank-algoritme zou rollen) bijvoorbeeld een uitstekend product in handen heeft. Uiteindelijk zou dit *entity search* bepaalde zoekqueries in Bing sterk moeten verbeteren. Ook nieuwe gebruikersinterfaces die uitgaan van de input van zowel een hand als een pen zouden in de toekomst nieuwe toepassing van Windows 8-tablets en aanraaktafels mogelijk moeten maken.

China was een unieke cultuurervaring, maar was vanuit een IT-perspectief niet bijzonder inspirerend. Korea was op alle vlakken een verrassing. Eén ding mag duidelijk zijn – het was een fantastische reis die eigenlijk iedere student een keer zou moeten maken. Op de volgende studiereis van Inter-*Actief*!

Figuur 2: Proppen in de metro van Seoul

KPN Consulting

Gids in de nieuwe wereld

Arnold van Mameren
Vice President KPN Consulting

Een gids zijn in de nieuwe wereld voor onze klanten en relaties: dat is de missie van KPN Consulting. Die gids kunnen ze alleen zijn wanneer ze onze mensen in staat stellen ook zélf een gids te zijn. Dat doen ze door ze los te laten, hen alle vertrouwen en verantwoordelijkheid te geven. Maar ook door ze te voeden met het beste van het beste: de meest interessante opdrachten, inspirerende opleidingen en – niet te vergeten – een bedrijfscultuur die staat als een huis én tegelijkertijd hun mensen vleugels geeft.

KPN Consulting is het ICT-adviesbedrijf van KPN, de marktleider voor geïntegreerde IT- en telecommunicatiedienstverlening in Nederland. De drijfveer van de consultants is gestoeld op een dertig jaar oude traditie van avontuur en enthousiasme. KPN Consulting heeft een kleurrijke historie: in 1980, aan het begin van het digitale tijdperk, begon het bedrijf als Pink Elephant, een bijverdienste van drie TU-studenten, aan een groot avontuur. Buiten collegetijden beheerden zij de mainframes van onder meer IBM, Dow Chemical en diverse ministeries. Overnames leidden tot diverse naamsveranderingen: via PinkRoccade naar Getronics Consulting. Sinds eind 2011 luidt de naam KPN Consulting, met vestigingen in Zoetermeer, Apeldoorn en Groningen.

Volgens Arnold van Mameren, vice president KPN Consulting, zijn de uitgangspunten niet beïnvloed door de vele naamsveranderingen. “De avontuurlijke instelling waarmee die studenten Pink Elephant runden, is bij ons nog steeds voelbaar. Wij introduceerden wereldwijd gebruikte standaarden ITIL en Prince2 in Nederland en zorgden hiermee voor een stevig fundament voor de hele ICT-sector. Met professionaliteit en de drive om nieuwe dingen te ontwikkelen bouwen wij verder aan de ICT van de toekomst. Daarbij is ICT geen doel op zich, maar een middel om klanten hun doelen te helpen realiseren. Sinds vijf jaar vormt onze kennis van ICT een mooie combinatie met de kennis van telecommunicatie binnen KPN. Wij willen vooruitstrevend zijn binnen het KPN-concern door voorop te lopen met de nieuwste technologieën. We zijn en blijven kwartiermakers.”

Een op een

Het is de corporate strategie van KPN om voor organisaties te fungeren als dienstenaggregator, vertelt Arnold. “KPN brengt diverse telecommunicatie- en IT-diensten samen, en klanten nemen uit de cloud die diensten af die ze op dat moment nodig hebben, waarbij ze betalen naar gebruik. Je ziet bovendien IT en telecommunicatie steeds verder naar elkaar toe groeien: toepassingen worden onderling uitgewisseld. Voorbeelden hiervan zijn Lync en Office 365 van Microsoft. In deze continu veranderende wereld zoeken mensen steeds opnieuw naar oplossingen om contact te leggen, samen te werken en ideeën uit te wisselen. Wij faciliteren dat.”

Figuur 1: KPN Consulting stelt de mens centraal

Arnold vervolgt: "De kernwaarden van KPN zijn Persoonlijk, Eenvoud en Vertrouwen. Wij vertalen dat binnen onze organisatie als volgt: Persoonlijk, doordat onze medewerkers een gids zijn voor onze klanten en hem of haar met inventieve toepassingen helpen om vanuit de oude wereld de nieuwe te betreden. Eenvoud, door de nieuwste technologieën te ontdoen van hypes en te vertalen naar zo praktisch mogelijke oplossingen in de organisaties van klanten. Vertrouwen, door te weten wat belangrijk is voor de klant en samen te zoeken naar de beste oplossing."

Veel ICT-dienstverleners hanteren een one-to-many-concept, waarbij een dienst aan meerdere klanten tegelijk wordt aangeboden. KPN Consulting is juist een one-to-one-aanbieder, bij wie de nadruk ligt op maatwerkoplossingen. Arnold vervolgt: "Onze klanten bevinden zich in de publieke, financiële en industriële markt, het onderwijs en de zorg. We kennen deze markten heel goed. We zitten er dicht op, om te begrijpen wat er bij onze klanten speelt en te kunnen optreden als vertrouwd adviseur. Doordat we hun bedrijfsprocessen kennen, kunnen we anticiperen op toekomstige ontwikkelingen in hun markt. KPN Consulting richt zich daarbij op de hele keten, van advies, ontwerp en implementatie tot beheer en support. We hebben onze kennis in 6 practices ondergebracht. Elke practice bestaat uit een aantal zeer ervaren consultants met daaromheen een flexibele schil van associates – van high potentials tot ervaren professionals - die zich ook met dat vakgebied bezighouden. Iedereen brengt eigen expertise in, waardoor we elkaar en vooral onze klanten helpen. Onze aanpak verbindt mensen, processen en technologie. Daar ligt onze kerncompetentie. Wij werken met de nieuwste technologieën, waarmee we onze klanten innovatieve diensten kunnen aanbieden die slim, accuraat en kostenbesparend zijn. Bij veranderingen in de organisatie staat de mens voor ons centraal: we vertalen de impact daarvan naar de bedrijfsvoering en de systemen, maar vooral naar het werk van mensen. Door middel van verandermanagement begeleiden we mensen van de oude situatie naar de nieuwe, met onze specialisatie 'People in Change'. Op een iets hoger abstractieniveau helpen we onze klanten om de oude wereld te verbinden met de nieuwe, bijvoorbeeld door middel van social media en cloudoplossingen."

Continue ontwikkeling

"Om de werknemers van onze klanten te kunnen begeleiden in verandering, moeten onze consultants zelf ook kunnen veranderen", aldus Arnold. "KPN Consulting is een community van gedreven professionals die de waarde van ICT begrijpen. Sociale, nieuwsgierige mensen die nieuwe technologieën vertalen naar toekomstbestendige en mensgerichte oplossingen. Kortom: een organisatie die met plezier en met visie op verandering voortdurend de nieuwe wereld wil ontdekken. Onze bindende factor is hartstocht voor ICT en voor wat het kan doen voor organisaties en de mensen die er werken. Op basis van wederzijds vertrouwen bouwen wij een duurzame, persoonlijke band op met onze klanten. Deze samenwerking is intens, en de lol is om klanten steeds weer te verrassen met oplossingen die beter zijn dan de klant zelf had bedacht. De persoonlijke ontwikkeling van onze consultants is een continu proces. Daar hechten we grote waarde aan en daar investeren we in."

Arnold besluit: "We hebben nu 1000 eigen medewerkers met opleidingsniveau wo of hbo-relevant, en ongeveer 150 externe professionals. De gemiddelde leeftijd schat ik op ongeveer 34 jaar. Onze recruiters zoeken continu de beste talenten op de arbeidsmarkt. Zo blijft ook onze organisatie voortdurend veranderen en blijft onze pioniersgeest intact."

"KPN Consulting is het ICT-adviesbedrijf van KPN, de marktleider voor geïntegreerde IT- en telecommunicatiedienstverlening in Nederland. De drijfveer van de consultants is gestoeld op een dertig jaar oude traditie van avontuur en enthousiasme. "

Over KPN Consulting

KPN Consulting is het ICT-adviesbedrijf van KPN. Als onderdeel van KPN zijn we toonaangevend in Nederland met geïntegreerde IT- en telecommunicatiediensten. Onze visie is dat ICT veel meer is dan de inzet van technologie. Het vergroten van de daadkracht van mens en organisatie staat bij ons voorop. Al decennia identificeren we nieuwe technologieën en vertalen deze naar toekomstbestendige en mensgerichte oplossingen. Oplossingen die helpen ambities en doelen te realiseren. Niet voor niets hebben we een eigen opleidingsinstituut: één op de drie ICT'ers in Nederland heeft bij ons een opleiding gevolgd. Met ruim 1000 gepassioneerde professionals en sterke wortels in de maatschappij, zijn wij de gids in de nieuwe wereld.

Vestigingen: Zoetermeer, Apeldoorn, Groningen

Info:
- www.kpn.com/consulting
- consulting.werkenbijkpn.com

//Column

Van de voorzitter

Van de veurzitter

Door: Pim Jager
Voorzitter Inter-Actief

Ten tijde van dit schrijven, ruim na de door de readactie opgelegde deadline, begint het hier in het mooie Twente goed koud te worden. Iedereen heeft zich weer in de dikke winterkleding gehesen en naar verluid is zelfs de eerste sneeuw alweer gevallen.

Gelukkig is van die kou in de kamer niks te merken. Waar de airco ons in de zomer lekker koel houdt, houden de aanwezige computers ons in de winter comfortabel warm. Naast die fysieke warmte is er in de kamer nog een andere soort warmte. Voor veel leden blijven de kamer en de bank de plek om gezellig samen te komen en op te laden na een zware nacht, even pauze te houden met een kopje koffie, of lekker te ontspannen aan het einde van de dag onder het genot van een biertje. Goed is het ook om te zien hoe behulpzaam we bij Inter-*Actief* nog steeds zijn. Of je nou met een vraag zit over een werkcollegeopgave, waar je het beste met je ouders uit eten kunt of welke keuzevak je het beste kunt doen; altijd zijn er mensen genoeg die je willen helpen. Dat maakt de kamer ook de ideale werkplek voor commissies. Wat je vraag ook is, van het reserveren van het Educafé tot het regelen van een symposiumlocatie, er is altijd wel iemand in de buurt die hier al ervaring mee heeft en nuttig advies kan geven.

Die aanwezigheid van vele ervaren hogerejaarsleden zijn wij als bestuur ook zeer gelukkig mee. Zonder hun waardevolle adviezen, ideeën en hulp zouden we met Inter-*Actief* niet alle mooie dingen kunnen doen die we nu doen. Als vereniging moeten we ons dan ook zeer gelukkig prijzen met hun betrokkenheid, als we naar de verenigingen om ons heen kijken zien we dat dat helaas ook anders kan.

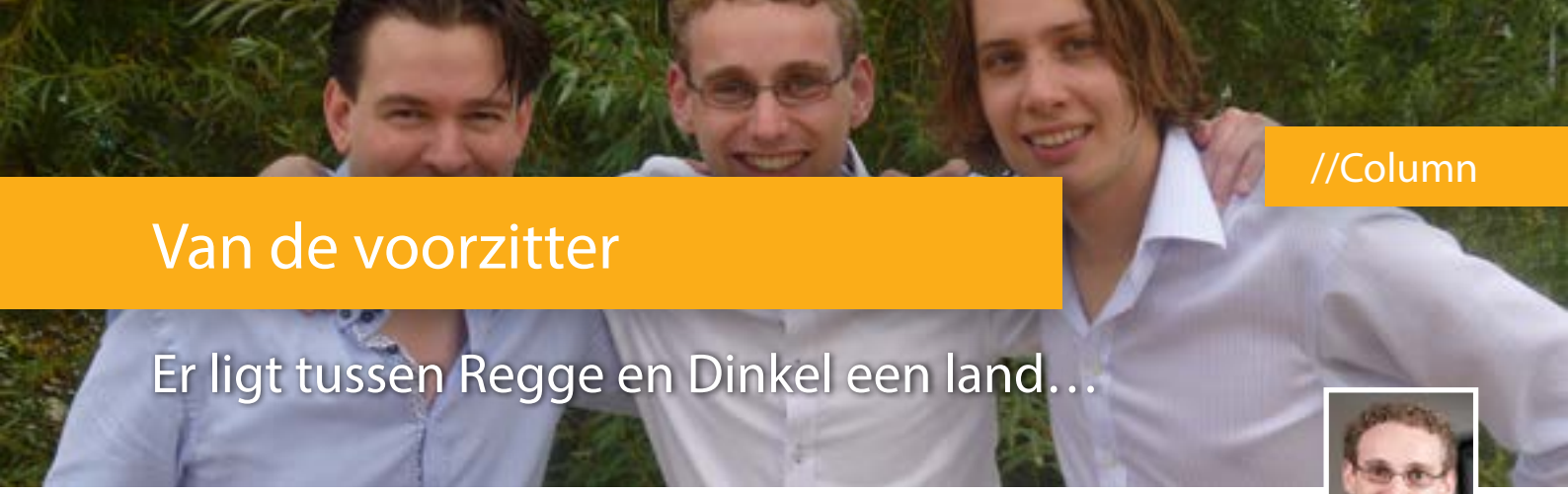
Als u dit leest zijn we alweer over de helft van het collegejaar en hard op weg naar de Dies en de halfjaarlijke ledenvergadering. Ook zal een aantal leden dat maar geen genoeg kan krijgen van de kou zich in Risoul gaan verstoppen voor 10 dagen sneeuwpret op de jaarlijke Winter-*Actief* skireis. Daarnaast zit het symposium er weer aan te komen, dit maal zelfs in landelijke variant. Onze zevenkoppige commissie heeft het afgelopen jaar keihard gewerkt om een prachtig symposium rond het thema 'smart surroundings' voor studenten uit het hele land te organiseren.

Ik zie u allen daar, en op de vele andere mooie activiteiten die wij met elkaar en voor elkaar organiseren!

Pim Jager opende voor de eerste maal zijn ogen op 29 augustus 1990 in het altijd bruisende Utrecht. Na een glansrijke carrière op basisschool de Zonheuvel in het immer gezellige Driebergen (incidenteel ook de plaats waar Pim tot zijn studie in Twente woonachtig is geweest) was het tijd voor de volgende logische stap en begon Pim aan zijn VWO-opleiding aan het Revius Lyceum in het pittoreske Doorn. Na zes jaar was duidelijk dat het VWO-onderwijshemweiniguitdagingmeer kon bieden en het tijd was voor een nieuwe uitdaging.

DezenieuweuitdagingvondPimaan de Universiteit Twente, na een wat moeilijk begin, waarin de verkeerde keuzes zijn gemaakt (de nasleep van deze keuzes zijn nog terug te vinden in zijn primair lidmaatschap bij E.T.S.V. Scintilla) zag hij na twee weken studeren alsnog het licht en schreef hij zich in bij I.C.T.S.V. Inter-Actief. Na onder andere te hebben gezeten in de ECie, Kick-IT, FlitCie, Cinema, TostCie en EWI-trip is het tijd voor de volgende stap. Hij mag zich sinds 4 mei dan ook kandidaat-voorzitter/intern noemen.

Inter-*Actief*



Van de voorzitter

Er ligt tussen Regge en Dinkel een land…

Door: Johan Noltes
Voorzitter ENIAC

En dat is het o zo mooie Twente. Voor alle lezers van de Vivat is het een vertrouwde regio, waarbij we allemaal ons eigen gevoel hebben. Toch vertrekken veel studenten na hun afstuderen uit Twente, om ergens anders aan het werk te gaan. Dat gold anderhalf jaar geleden ook voor mij. Dan valt het pas op dat er veel westerlingen zijn die niet zo vaak in het oosten komen, en de omgeving dus ook niet goed kennen.

Laatst bezocht ik bijvoorbeeld met mijn collega's een activiteit in de buurt van Deventer (natuurlijk geen Twente, maar nog wel in Overijssel). Enkele collega's – geboren en getogen in Noord Holland – waren zowaar verbaasd over het feit dat er snelwegen naar Twente leidden, dat er snel mobiel dataverkeer beschikbaar was, en dat er ook nog spoorwegovergangen met slagbomen zijn. Op mijn beurt was ik weer verbaasd over hun blijkbaar gebrekkige kennisniveau. Overigens waren ze wel gecharmeerd van de prachtige kleuren in het Overijsselse landschap. Een beetje afwisseling is dus zeker de moeite waard, en houdt de geest scherp.

Dat is dan ook de reden dat ENIAC probeert om haar activiteiten op wisselende plekken in het land te organiseren. Na de Olympische waterbaan in Zoetermeer en het strand van IJmuiden volgt op 2 februari de ALV en informele activiteit in het vertrouwde Enschede. Tijdens de ALV kijken we terug op het afgelopen jaar, maar belangrijker: we praten ook over de toekomst van ENIAC. Het bestuur heeft de afgelopen anderhalf jaar een aantal activiteiten opgezet, die positief zijn ontvangen door onze leden. We kijken tevreden terug op het resultaat van bijvoorbeeld de informele activiteiten, het jaarboek, de Scriptieprijs, en het Scholarship.

Het opzetten van deze activiteiten heeft echter meer inspanning gekost dan verwacht. Daarom willen we dit jaar een deel van onze activiteiten gaan overdragen aan commissies. Om de werkdruk te verlagen, maar ook vooral om de continuïteit te bewaken. Gezien het succes van de afgelopen activiteiten maken we ons daarom ook geen zorgen over het vinden van mensen die plaats willen nemen in de commissies. Meld je dus gerust aan bij het bestuur om actief te worden voor de vereniging.

Ook voor de opleiding Informatica komt er een bijzonder jaar aan. Dit jaar start de Universiteit Twente met het Nieuwe Onderwijs Model. Kennis wordt niet meer overgedragen in vakken, maar in modules. Deze modules zijn nog volop in ontwikkeling, en daarbij wordt ook de input van alumni gewaardeerd. Zeker omdat er nu ook een accreditatietraject voor de opleiding loopt, waarbij ENIAC deels ondersteunt. Heb je dus een mening over de opleiding, bijvoorbeeld in relatie tot je huidige werk, neem dan contact op met ENIAC of de opleiding. We zien elkaar in Twente!

Johan Noltes, voorzitter

Johan Noltes is voorzitter van ENIAC: de ENschedese Informatica Alumni Club. ENIAC is de alumnivereniging voor oud-studenten Informatica, bedrijfsinformatietechnologie en Telematica aan de Universiteit Twente.

Voor slechts € 5,- per jaar kan je al lid worden van deze club. Je krijgt dan in ieder geval de Vivats die jaarlijks verschijnen (meestal zo'n 4 stuks, maar niet helemaal per kwartaal) en uitnodigingen voor de activiteiten die we organiseren (meestal per mail). Daar mag je dan vervolgens (veelal gratis!) aan deelnemen. En al doe je maar eens in de paar jaar ergens aan mee, die € 5,- kan toch bijna iedere informatica-alumnus wel missen? Zo houd je toch nog wat binding met je wetenschappe- lijke roots en af en toe contact met vrienden uit je studietijd.

Johan Noltes
voorzitter@eniac.utwente.nl

//Advertorial

Trends & Hypes: NFC

Een elektronische kluis in je smartphone

Door: Willem de Boer
Senior Consultant bij Technolution B.V.

Een elektronische kluis in je smartphone om bankpassen en wachtwoorden op te slaan. Dat kan met NFC, waarmee je legio toepassingen aan de telefoon toevoegt. Veilig, handig en flexibel.

Zou het niet mooi zijn als je de collectie pasjes in je portemonnee zou kunnen samenvoegen tot één universele pas? Een elektronische pas die wordt geïntegreerd in je smartphone. Om te betalen steek je niet meer een bankpas in een apparaat, waar je moet wachten, pinnen en nog eens wachten. Straks veeg je met je smartphone langs een terminal en de betaling is verwerkt. Net zo snel als we nu al in- en uitchecken in het openbaar vervoer.

Intrinsiek veilig

De technologie om dit te realiseren heet Near Field Communication (NFC). Bedacht in de jaren negentig door Philips en Sony, met als doel een smartcard te integreren in mobiele apparatuur. NFC borduurt voort op RFID, dat al enkele tientallen jaren wordt gebruikt als passieve identificatiechip. Door deze technologie in een telefoon te stoppen, krijg je voeding en extra communicatiekanalen tot je beschikking. Zo ontstaat een veel intelligenter product. NFC is een standaard voor draadloze communicatie die alleen op korte afstand werkt (tot 10 cm). Daarmee is al een eerste veiligheid ingebouwd: je moet bewust je telefoon dicht bij een reader brengen om te kunnen communiceren.

Toepassingen NFC

NFC is breed te gebruiken. Betalen en ticketing zijn twee toepassingen waar de hele wereld naar kijkt. Maar ook toegangscontrole, zowel fysiek als online, en identificatie liggen voor de hand. Een veeg langs een Swipe-Tag en de deur gaat open of je mobiel krijgt toegang tot een beveiligd netwerk. Via NFC worden sleutels, apparaatsettings en veiligheidsinstellingen uitgewisseld. Zo kan een Swipe-Tag in schouwburgen bij de entree toegang geven en de instellingen van je telefoon aanpassen naar het profiel 'stil'.

Elektronische kluis

Allemaal toepassingen die zijn terug te voeren op informatie-uitwisseling via NFC: instellingen van apparatuur, financiële of persoonlijke gegevens, wachtwoorden. Stuk voor stuk gevoelige informatie waar NFC veilig mee omgaat. Want een tweede sterke troef van NFC is versleuteling (encryptie) en 'verstoppen'. Een NFC-chip is erg goed in het bewaren van sleutels, iets waar de meeste andere chips op een telefoon moeite mee hebben. NFC is daar juist specifiek voor ontworpen. De NFC-chips worden geleverd met een sleutel aan boord. Maar de gebruiker kan zelf ook sleutels opslaan in de NFC-chip, die zo te gebruiken is als een soort kluis.

Juist die kluis is een reden waarom grote marktpartijen heil zien in NFC: banken, telecomproviders en aanbieders van diensten en producten verwachten veel van NFC. In de toekomst zullen we allerlei 'security credentials' gaan bundelen op onze telefoon: bankpassen en al die andere pasjes in je portemonnee, maar ook wachtwoorden voor allerhande websites en internettoepassingen.

Security: telefoon als onderdeel in twee-factorauthenticatie

Een NFC-telefoon heeft hetzelfde veiligheidsniveau als de huidige pinpas die we volop gebruiken. Toepassingen waarbij beveiliging is vereist, zullen altijd met een twee-factorauthenticatie werken: een controle met twee elementen. Iets wat je hebt: de telefoon, en iets wat je weet: een wachtwoord of pincode. Alleen met die combinatie krijg je toegang tot een site of dienst. Iemand anders kan niet veel met jouw telefoon, evenmin als nu met je pinpas.

Wachtwoord is passé

De één-factorauthenticatie met naam en wachtwoord die we nu nog op vrijwel alle websites hanteren, is een aflopende zaak. Technieken om zulke combinaties te hacken worden alleen maar beter. Een beetje hacker kraakt een wachtwoord van 15 tekens binnen een dag. Een veilig wachtwoord moet dus al meer dan 15 karakters hebben, liefst met wat random karakters. Dat is niet meer te onthouden.

Daarom zal er een enorme toename zijn in twee-factorauthenticatie, waarbij je naast een wachtwoord ook een fysieke controle hebt met een device. Je wilt straks niet voor elke dienst een ander apparaat bezitten. Het is veel handiger om alles samen te brengen op de smartphone. NFC kan deze gegevens ook nog veilig opslaan. Het uploaden van credentials naar de veilige NFC-kluis kan via het veilige NFC-kanaal of via 3G vanaf een backoffice. Dat zijn communicatiekanalen die doorlopen tot in het veilige gedeelte van NFC.

Telecomprovider & trusted third party

Niet iedereen kan of mag zomaar sleutels in de NFC-chip zetten. De NFC-chip is gekoppeld aan de simkaart van het toestel. De provider van wie je de simkaart koopt, beheert ook de NFC-chip. Deze partij heeft de moedersleutel en biedt een versleuteld kanaal om andere sleutels en applicaties in jouw NFC-kluis te plaatsen, bijvoorbeeld een betaalsleutel van de bank. Het is voor de bank veel werk om met elke provider apart afspraken te maken en datzelfde geldt voor de providers. Daarom is een overkoepelende organisatie nodig. Een 'trusted third party' waar providers zich bij kunnen aansluiten, zodat de banken en providers maar met één partij zaken hoeven te doen. Zoiets als wat Interpay is voor de pinbetalingen.

Waarschijnlijk komt er zo'n internationale derde partij. Dan is de cirkel rond en kunnen aanbieders van diensten, zoals banken, winkels en (internet) diensten, via één partij hun sleutels distribueren naar NFC-telefoons. Organisatorisch is dat een grotere uitdaging dan technisch.

> "Niet iedereen kan of mag zomaar sleutels in de NFC-chip zetten"

Veiligheid dankzij cirkels

Over cirkels gesproken: die zijn in security altijd heel erg goed. Bij NFC is ook de beveiligingscirkel rond: de NFC-betaalterminal staat in verbinding met een backoffice die de transacties registreert en sleutels aanlevert en de mobiele telefoon is verbonden met zijn eigen backoffice, bijvoorbeeld de bank. De telefoon en terminal zijn met elkaar verbonden via het NFC-protocol. Maar ook beide backoffices kunnen met elkaar praten. Zo is een cirkel ontstaan en is de security gewaarborgd. Op meerdere fronten kun je de transactie valideren, dat kan met een bankpas niet. Dit securityaspect is nu nog onderbelicht in de promotie van NFC, maar dat is juist een heel sterk argument. Het biedt een extra kanaal voor controle bij betalen, het kopen en gebruiken van tickets of bij internettoegang.

Figuur 1: Door NFC kan dit verledentijd worden.

Veiligheidswedloop

De NFC-chip zelf is net zo veilig als smartcards (in bankpassen). En ja, die zijn te kraken. Er is een eeuwige wapenwedloop tussen chipbouwers, hackers en laboratoria die via 'reverse engineering' zo'n chip ontleden. Je zult dus om de drie á vier jaar een nieuwe chiptechnologie moeten invoeren om nieuwe aanvallen te weerstaan. Ook daarom is de mobiele telefoon een goed platform, aangezien de gemiddelde gebruiker één á twee jaar met zijn telefoon doet. Dus is het een perfect platform om die roulatie en vernieuwing bij te houden.

NFC biedt volop kansen

NFC is een trend. Betalen en ticketing zijn twee toepassingen waar de hele wereld naar kijkt.

Maar ook bij toegang verstrekken tot internet en fysieke toegangscontrole liggen volop kansen voor technologieontwikkelaars. Partijen die al kennis hebben van het ontsluiten van mobiele systemen richting centrale systemen, zullen NFC snel weten toe te passen. NFC is een kans voor nieuwe technologische ontwikkelingen. Zakelijk en privé zullen we steeds meer tokens krijgen om in te loggen en te betalen. Met NFC kan dat op één device, ideaal dus! De grootste uitdaging is nog de veilige distributie van sleutels. Zodra dat goed georganiseerd is, zijn er overal tal van mogelijkheden met NFC.

Topicus

Door: Harald Dannenberg
Directeur Topicus Care

Harald Dannenberg, geboren en getogen in Rijssen, is nu Directeur bij Topicus Care. Als 6e medewerker van het almaar in cellen opsplitsende bedrijf met Twentse roots, behoort hij wel tot de oude garde. Inmiddels Directeur van de cel Topicus Care en verantwoordelijk voor 22 werknemers.

Kan je iets meer vertellen over wie je bent?

In 1997 begon ik met mijn opleiding BIT (Bedrijfsinformatietechnologie), toen BIT nog maar vier jaar bestond. In 2001 studeerde ik af en begon met het verkennen van de arbeidsmarkt. De periode viel samen met de aanslagen in New York op 11 september, hierdoor was de arbeidsmarkt in rep en roer. De detachering zakte in elkaar. Daarbij waren dit niet de soort bedrijven waar ik naar op zoek was. Het werken in een team vind ik belangrijk en wanneer je telkens bij een andere klant werkt is het lastig om een hecht team te vormen. Dat was mijn beeld.

Hoe ben je bij Topicus terechtgekomen?

Tijdens mijn afstuderen bij Essent heb ik me bezig gehouden met onderzoek naar internetgebruik. In die tijd (in 2001) stond het gebruik van internet nog echt in de kinderschoenen. ADSL was in opkomst en mijn onderzoek ging onder andere over de vraag: “Hoe moet je een serverpark om laten gaan met deze groei?” Hiervoor heb ik een model opgesteld en doorgerekend. Waar uiteindelijk een advies uitkwam naar Essent. Hier kwam veel techniek bij kijken, maar heb daar nooit voor moeten programmeren. Echt 120% een BIT opdracht. Dit wilde ik wel vaker doen.

Tijdens de diploma-uitreiking in 2001 hield Leo Essink, medeoprichter van Topicus en oud-docent informatica op de UT, een enthousiast verhaal over de werkzaamheden van Topicus. Na mijn onderzoek naar het gebruik van internet pasten de werkzaamheden van Topicus als een jas. Diezelfde middag keek ik nog op de site van Topicus en stuurde ik mijn sollicitatie. Drie weken later was ik werkzaam als programmeur bij Topicus. Ik begon als programmeur om de techniek beter te leren kennen, waarbij ik begon met een aantal projecten voor financiële dienstverleners. In de studie heb ik wel wat Java en functioneel programmeren gehad, maar eigenlijk had ik niet zo veel ervaring op technisch vlak.

Hoe ben je verder gegroeid binnen Topicus?

Programmeren deed ik voor een jaar om mijn technische kennis te verbeteren. Na een jaar kreeg ik de rol van analist en ik werd in 2004 projectleider. Tot die tijd was Topicus vooral bezig met projecten in de financiële sector, in 2004 hadden we nog zo’n 30 medewerkers. We waren bezig om onze activiteiten uit te breiden naar de zorg en onderwijssector. In die tijd is de beroemde cellencultuur van Topicus ontstaan en was daar de eerste opsplitsing: Topicus Zorg. In de zorgsector zijn we toen begonnen met het ontwikkelen van een HIS (Huisarts Informatie Systemen). Ik begon als projectleider van diverse zorgprojecten. Na de zogenaamde medische systemen volgden vrij snel de niet-medische toepassingen binnen de zorg, zoals Thuiszorg en Jeugdzorg. Hierdoor splitste Topicus Zorg zich in drie onderdelen, namelijk Topicus Cure, Care en Jeugdzorg. Ik werd directeur van Topicus Care, waarbij we ons richten op de domeinen Verpleging, Verzorging en Thuiszorg, GGZ (Geestelijke en gemeentezorg.

Hoe kijk je naar de toekomst?

Bij de overheid liggen nog mogelijkheden voor Topicus. Dat is een nieuw gebied voor ons dat wij zeker gaan verkennen. Wij zijn voornemens om vanuit onze vestiging in Enschede een platform voor gemeenten te lanceren voor coördinatie van zorg bij burgers en gezinnen, met mobiele ondersteuning voor wijkteams. Daar zal ik mij actief mee gaan bemoeien.

Wat is mooi en wat is slecht aan Topicus?

De enorme groei in de afgelopen jaren, het was geweldig om hier deel aan te nemen. Nu heeft Topicus 350 medewerkers en 8 vestigingen. Daarentegen brengt zo’n grote organisatie ook nadelen. Je moet dingen formaliseren, dit botst af en toe. We worden geconfronteerd met regeltjes en dat brengt interessante discussies naar boven. Daarbovenop komt nog de druk van buitenaf, van verschillende grote organisaties die ons beter in de gaten gaan houden. Hierdoor moeten we audits laten uitvoeren van buitenaf. Om te ondernemen wil je de vrijheid hebben om te doen en laten wat je wilt, dat gaat soms niet in zo’n grote organisatie. Mensen bij Topicus zijn van nature gedreven, dan zijn regels eigenlijk noodzakelijk kwaad.

Niet dat Topicus nu een grote, logge organisatie is geworden. Integendeel, de verschillende units zijn net kleine bedrijven en er heerst een open en informele cultuur. Je hebt je eigen verantwoordelijkheid en daar wordt je op aangesproken. Dit is heel persoonlijk en maakt iedere dag weer boeiend om voor Topicus te werken.

Bedankt voor het interview!

VOLGENDE KEER IN I/O VIVAT

- West vs. Oost – de Macht over het Internet
- Steganografie
- Rondje Zilverling

ADVERTENTIE

QUIN_WERVING_AD_A4_WERKEN-LEUKER