

Bescherming digi-identiteit escaleert tot wapenwedloop

Jagen op anonus

Met wie en waarover we converseren, is iets heel persoonlijks. Al sinds het briefgeheim houden we onze correspondentie dus voor anderen verborgen. Exploitanten van communicatiemiddelen willen echter juist zo veel mogelijk over hun klanten weten. De jacht op anonus is geopend.

DOOR JACOB VAN KOKSWIJK

Van oudsher is er spanning tussen het individu en zijn omgeving. Het individu wil af en toe zijn identiteit wil verhullen. De omgeving (groepen, bedrijven, ordehandhavers, overheid) die wil weten wie de onbekende is en zijn identiteit dus wil vaststellen en registreren. Daar probeert de gezochte dan weer onderuit te komen.

Maskers, vermommingen, pseudoniemen en bijnamen komen overal ter wereld voor. Identiteitswisselingen zijn vaak gebonden aan culturen of festiviteiten, elk volk heeft daarin zijn traditie. Denk aan ons carnaval, het Karagözspel en de kleurige processies van als dier of god verklede mensen. De Grieken hadden de gemaskerde blijspelen, Egyptenaren de poppensatire, en de Romeinen vierden het feest van de saturnaliën met vermommingen en optochten. Velen kennen de Wajangpoppen die gebruikt werden om mythen en moralen aan de orde te stellen.

Voor sommigen waren de verkleedpartijen reden om de wet te ontduiken. Vandaar dat de overheid regels ging stellen: "In verband met de openbare orde, zeden, rust, veiligheid, reinheid en gezondheid en vanwege hinderlijke gedragingen is het verboden op het openbare domein en in publiek toegankelijke plaatsen het gelaat zodanig te bedekken dat de identificatie van de persoon onmogelijk is." Desalniettemin

gebruiken talloze mensen op zijn minst een alias en meet de overheid zelf diplomaten, spionnen en achtervolgden een nieuwe identiteit aan.

Geschiedenis

Technologie helpt ons om onze identiteit effectief te klonen. Na de uitvinding van de telegraaf werd de wereld omspannen met draden. Daarmee werden berichten, die bij het ene postkantoor afgegeven waren, overgeseind naar een ander kantoor, vanwaar ze als een soort van brief werden bezorgd bij de geadresseerden. De telex bood meer mogelijkheden voor individueel point-to-point berichtenverkeer. Na de vondst van de facsimile werden berichten van het ene naar het andere apparaat overgeseind alsof het foto's waren, waarna de geadresseerde ze ter hand gesteld kreeg.

De draadtelefoon verbond een toestel met telefoons in een andere straat of complex, waar een nieuwsgierige passant dan de telefoon opnam en vervolgens op zoek moest naar de persoon voor wie het gesprek was bedoeld. Hetzelfde gebeurde op Arpanet, de voorloper van het internet, waar draadverbonden computerinstallaties informatie uitwisselden en elke medewerker de terminals kon gebruiken. Via subadressen werden persoonlijk gerichte berichten naar de juiste terminal gestuurd. Tot circa 1998 was het internetverkeer nog steeds nagenoeg anoniem.

Sinds het begin van de elektrische en elektronische communicatie is het aantal identiteiten dat we hebben veelvoudigd. Ieder van ons heeft meerdere telefoonnummers en verschillende e-mailadressen. Moderne commu-

nicatiewijzen hebben andersoortige relaties tot gevolg, zowel in individueel kader als in groepsverband. Deze nieuwe relationele contacten leiden in bedrijven ook tot andere manieren van samenwerken. Na de publieke introductie van het internet zijn overheid, bedrijfsleven en individuen mee gaan doen aan de identiteitsverandering. Virtuele omgevingen, zoals Entropia en Second Life, creëren zelfs een alternatieve wereld waar digitale afbeeldingen van personen (avatars) en subbrands van bedrijven een tweede leven leiden. Daarmee is de unieke identiteit vervallen.

Maakbaar 'ik'

Aanvankelijk versierde men zichzelf met kleding en kleurstof. In de twintigste eeuw kwamen daarbij het gebruik van cosmetica, gekleurde lenzen, orthodontie, plastische chirurgie en fotomontage. De maakbaarheid van mensen nam door multimedia- en computertechnieken een snelle vlucht. Met digital signal processing (DSP) en samplingtechnieken kan je een stem naar wens aanpassen. Notatieprogramma's op de computer maken muzikale composities populair en easy listening. Gezichten worden eenvormig en publieksaantrekkelijk met morphingtechnieken. Als paspoorten moeilijker te vervalsen zijn, dan passen we de mens aan. Vandaar de toevoeging van biometrische kenmerken, die ook niet feilloos blijken te zijn.

De boodschap van het internet is even simpel als eenduidig: 'creëer je eigen werkelijkheid'. Het web is uiteindelijk een do-it-yourselfwereld. Dat zien we bijvoorbeeld bij het vormgeven van

.....
Iedereen heeft werk- en
privételefoon



De Samsung B5702 heeft plaats voor twee simkaarten. Hiermee kan iemand twee identiteiten aannemen: de ene voor als de baas belt, de ander voor als de minnares aan de lijn hangt. (Photo by courtesy of Samsung Electronics. Source: www.techblog.gr.)

de identiteit. In de fysieke wereld zijn het lichaam, en de etnische, raciale en sociale achtergrond bij de geboorte van een mens bepaald. In het virtuele domein kun je die naar believen vaststellen. Met die maakbare identiteit kan men zich levensecht anders positioneren, het is een soort makeover

van jezelf. De attributen die iemand voor zichzelf kiest, hoeven niet overeen te komen met de eigenschappen van degene die zich fysiek voor het computerscherm bevindt. De pasgeboren persoonlijkheid kan vervolgens chatten met anderen in die virtuele ruimte. Daarmee is hij via sociale interactie

verwikkeld in een continu proces van identiteitsconstructie.

Decentralisatie

Deze virtuele ruimten geven de gebruikers simpel de kans om te spelen met hun identiteit en uiterlijk en om persoonlijkheden uit te proberen. Wie in meerdere ruimten verschillende identiteiten creëert, decentraliseert niet alleen zichzelf, maar kan zich ook grenzeloos vermenigvuldigen. Er bestaat immers geen limiet aan de virtuele ruimten waarin iemand hoe dan ook kan optreden. Elektronische contactplatforms en chatrooms zijn in die zin proeftuintjes waarin mensen kunnen ontdekken wie zij zijn of zouden willen zijn. De jongste generaties kunnen zich in meerdere identiteiten naast en los van elkaar manifesteren. Vroeger noemden we dat persoonlijkheidsstoornis, nu is het een softwareapplicatie. In bepaalde situaties sluit men zelfs fysiek de ontvangst af om van de ene identiteit over te stappen op de andere. Iemand logt bijvoorbeeld uit wanneer hij online is en logt daarna weer in onder een andere nickname. Anderen gebruiken een speciaal e-mailadres of 06-nummer en laten dat verlopen wanneer ze een bepaalde alias niet meer gebruiken. Door de automatische reset sterft die na enige maanden vanzelf een virtuele dood. Het negeren van oproepen op een oude identiteit is voor de jongere generatie een manier om vooruit te zien.

Het hopen tussen belevingswerelden roept gevoelens van maakbaarheid op: 'als de ene wereld niet leuk is, ga dan even in de andere kijken.' Tijd en identiteit krijgen een manipuleerbaar karakter. Je hoeft in die andere wereld jezelf niet te zijn, of je kunt juist jezelf zijn. Een inwoner van het internet kan de tijd verzetten, spelen met tijdzones, timers beïnvloeden enzovoort. Bij elke tijd hoort een andere identiteit, en als de tijd verandert, verandert die mee.

Overheden en bedrijven hebben het nu al moeilijk om de databanken te zuiveren van burgers met *niemand@nergens.nl* als e-mailadres en die wonen in Afghanistan, het eerste land in de aanklikbare alfabetische reeks. E-government is het realiseren van een overheid die via elektronische weg met haar onderdanen contact houdt. De inspanningen hiervoor zijn nutteloos, wanneer burgers naar willekeur staatsburger of stateloze burger kunnen zijn, of zich ongemerkt voordoen als een andere burger. Hoe wil je de over-

heid een virtuele samenleving regeren, als zij niet eens weet wie de bewoners ervan zijn? Het standaardinstumentenarium van de publieke en private sector voldoet niet. Grenscontroles en handboeien helpen niet bij een virtuele mens.

Persoonlijke nummers

Bij telefoon en internet gaat de techniek ervan uit dat een contact van mens tot mens verloopt van apparaat naar apparaat oftewel terminal to terminal. De communicatietechnologie is ingericht om elke bestemming een nummer toe te kennen. Ieder terminaldevice heeft een adres in de vorm van een reeks hexadecimale karakters. Voor de gebruiker is dat zichtbaar als een reeks cijfers, een nummer, soms vertaald in een letterbeeld (URL, domeinnaam of e-mailadres). Een mens met meerdere communicatieapparaten heeft dus ook meerdere communicatieadressen. Er is dus geen rekening gehouden met identiteit van en de relaties tussen de personen achter die terminals. Mensen maken dat onderscheid wel. Het eerste verschil is pragmatisch: werk en privé. Het tweede: bekenden en vreemden. Kennelijk houdt het scheiden van nummers verband met het verbergen van identiteit. De mens is geen nummer, of wil geen nummer zijn. Het was te verwachten dat ze anders met de codes zouden omgegaan dan de innovators hadden bedacht.

In de westerse wereld heeft bijna iedereen voor elke relationele omgeving een apart telefoonnummer en vaak ook een verschillend e-mailadres. Telefoonnummers en e-mailadressen voor werk- en privé scheiden we bewust. Veel mensen houden er nog meer nummers en adressen op na. Enkele pogingen om deze adressen samen te brengen tot één persoonlijk nummer (unique personal number of unified messaging) zijn na een snelle opkomst aan het eind van de vorige eeuw een stille dood gestorven. Alhoewel, in Nederland heeft een dergelijke dienst voor persoonlijke nummers via Edutel wel voet aan de grond gekregen bij bepaalde beroepen.

Ontmaskeraars

De conversie van een telefoonnummer naar een IP-nummer (telephone number mapping, ENUM) werkt op basis van een translatiemodel, dat het telefoonnummer omzet in een IP-adres of vice versa. Hierdoor komt de convergentie en integratie van telefonie

Identificatiegetallen

Zoals de computernetwerkmodule een uniek MAC-adres kent, hebben mobiele telefoons een international mobile equipment identity (IMEI). Dat is een meestal 15-cijferig nummer waarmee een gsm te identificeren is. Het is te gebruiken om het toestel te laten blokkeren bij verlies of diefstal en om een mobiele telefoon te locken of unlocken. Dit getal is op te roepen door achtereenvolgens *#06# in te toetsen op de mobiele telefoon, waarna het verschijnt in het display. Steeds meer apparaten geven na het controlecijfer nog een software version number (SVN), dat de softwareversie aanduidt. De 16-cijferige combinatie van IMEI plus SVN heet het international mobile station equipment identity and software version number (IMEISV). Daarnaast bevat de sim nog een international mobile subscriber identity (IMSI), als uniek nummer verbonden aan elke GSM- en UMTS-gebruiker van mobiele telefoons. Het is opgeslagen op de sim in de telefoon en wordt door de telefoon naar het netwerk van de telecomaandbieder gestuurd. Het doet ook dienst om andere gegevens over de mobiel te verkrijgen uit het home location register (HLR). Het IMSI-nummer is maximaal 15 cijfers lang. De eerste drie cijfers staan voor de mobile country code, gevolgd door 2 cijfers (in Europa) of 3 (in Noord-Amerika) voor de mobile network code. De navolgende cijfers vormen het mobile subscriber identification number dat de telecomaandbieder gebruikt om de afnemer van telecomdiensten te identificeren. Om af luisteren van het IMSI-nummer te bemoeilijken, verstuurt de telefoon dit nummer zo min mogelijk. In plaats ervan gebruikt het een temporary mobile subscriber identity (TMSI), dat willekeurig gegenereerd is.

en internet naderbij. Ook IP-telefonie kent een protocol voor de integratie van telefoon- en internetfunctionaliteiten: SIP. Unified communications, momenteel een buzzword, is in feite een softwaretoepassing die alle verschillende vormen van elektronische communicatie weer naar één persoon leidt. Serviceproviders proberen met alle mogelijkheden vat te krijgen op de identiteit van de gebruiker. Prepaidbellers ontvangen bonusgeld als ze invullen wie ze zijn en waar ze wonen. Het gebruikersprofiel vertelt waar ze hebben gebeld, wanneer en met wie. Internetsites identificeren hun bezoekers door ze zich verplicht te laten inschrijven voor ze kunnen inloggen. Het internet is daarnaast in de afgelopen jaren steeds meer dichtgetimmerd door geografische en technische identificatiekenmerken toe te voegen aan het berichtenverkeer en aan de gebruikte terminal (MAC-adres, IMEI-code en dergelijke).

Daarmee sluit het net zich om de anonieme gebruiker. Zal het weldra onmogelijk zijn te verbergen wie je bent? Net zoals sommige bonuskaarthouders proberen telecomgebruikers zich aan die identificatie te onttrekken. Het wisselen van 06-sims komt voor onder jongeren en criminelen. Internetters werken met een proxy of anonymizer. In ieder mens schuilt een tweede ik, dus meerdere identiteiten zullen blijven. Al is het maar door in elke broekzak een andere telefoon mee te dragen.

Door tekstanalyse en gedragskenmerken kunnen forensische experts de identiteit van de zich anoniem wanende beller of internetter achterhalen. Met het IP-adres van een computer of met een driehoeksmeting tussen de zend-

masten kunnen zij bepalen waar het toestel zich bevindt, maar niet wie het bedient. Bij telefoongesprekken wordt stemanalyse steeds vaker als authenticatie gebruikt. Bij teksten past men datamining toe, waarmee karakteristieke elementen in de communicatie zijn te herkennen. Brieven met doodsbedreigingen of bommeldingen werden al nauwkeurig nageplozen op aanwijzingen die de identiteit van de dader kunnen onthullen. Sinds enige jaren bestaan er applicaties die weten te onderscheiden of een man of vrouw de tekst heeft geschreven. Met informatie-extractie en textmining doorzoekt men het web, gebruikmakend van de modernste technieken voor de verwerking van natuurlijke taal. Maar lukt dat ook met IRC en sms-taal? Een sms'je is doorgaans niet langer dan 160 tekens. Eerst leek het dat hoe korter de tekst was, hoe minder aanwijzingen hij bevatte. Sinds kort kan echter ook de analyse van sms-berichten de identiteit van een afzender onthullen in onder meer cyberstalking- en moordzaken. Deze nieuwe vormen van biometrie leggen de hand op identiteit 2.0.

Jacob van Kokswijk (tm@kokswijk.nl) is hoogleraar aan de Katholieke Universiteit in Leuven, parttime ICT-consultant bij Caggemini, veelgevraagd spreker bij congressen en lid van de stuurgroep Next Generation Networks Initiative van de EU.