01/2012

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 1 - 2012

EEN VIRUS IN JE NOODSTROOMGENERATOR

HACKEN IS GEEN OPSPORINGSBEVOEGDHEID!

EXPLOSIEVE GROEI VAN ANDROID MALWARE

QIY DRAAIT DE DIGITALE WERELD OM

IDENTITY NEXT

TSTC – de Security Opleider van Nederland

De wereldwijde lancering van
Computer Hacking Forensic Investigator

NIEUW

CHFI v8

vindt in de Benelux exclusief plaats bij TSTC van 5 - 9 maart 2012.
Neem contact op via info@tstc.nl voor uw speciale "launch" aanbieding.

Certified Virtualization Security Expert (CVSE)
Certified VOIP Professional (ECVP)
Certified Risk Manager ISO 27005/31000
Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator (CHFI)
Certified Security Analyst (ECSA)
Licensed Penetration Tester (LPT)
Certified Secure Programmer (ECSP)
Disaster Recovery Professional (EDRP)
Certified Information Systems Security Professional (CISSP)
Certified Information Security manager (CISM)

Fast Track - een andere kijk op training en certificering!

Met eigen trainers, een afwijkende trainingsfilosofie
en natuurlijk onze unieke slagingsgarantie.

Circle of Excellence ATC EC-Council 2007
Circle of Excellence ATC EC-Council 2008
Circle of Excellence ATC EC-Council 2009
Circle of Excellence ATC EC-Council 2010
Circle of Excellence ATC EC-Council 2011

TSTC - 5 jaar op rij de beste EC-Council Security Opleider Benelux

TSTC TSHUKUDU TECHNOLOGY COLLEGE

Want security start bij mensen!!

WWW.TSTC.NL

VOORWOORD

Cyberscams en spam. Bestond het tien jaar geleden nauwelijks, het is nu een onderdeel van het dagelijks leven. Detecteren wordt steeds moeilijker. Was ik ooit overtuigd dat een filter niet nodig is, nu ben ik blij dat Google en Xs4all een eerste poging doen. Ik vind het leuk om te kijken hoe knullig deze pogingen soms zijn. Even later schud ik meewarig mijn hoofd als ik zie wat er wél doorkomt. Tegenwoordig zit er toch af en toe iets tussen waarvan ik denk: "Het is dat ik weet dat het niet echt is, maar onder bepaalde omstandigheden had ik daar wel op kunnen klikken." Zeker omdat bedrijven waar ik diensten van afneem, over belangrijke zaken zo'n tien jaar geleden via de gewone post communiceerden. Dat is óók voorbij. Detectie is niet meer zo simpel als: "dat zouden ze me nou nooit per email vragen."
Ik geef ook nog wel eens (on)gevraagd advies aan familie en vrienden. Ik probeer daarbij de FUD (fear, uncertainty, doubt)-factor laag te houden. Als je net je eerste schreden in het cyberwoud zet, geniet je nog niet van het natuurschoon. Het laatste dat je nodig hebt, is dat iemand je waarschuwt tegen 'lions, tigers and bears'. Ik zie ze liever veilig de smaragden stad ontdekken. Toch merk ik soms dat door mijn waarschuwingen een automatische software upgrade niet werd uitgevoerd. Uit angst dat het malware betrof. Of dat een zakelijke mail verworpen was als spam. Was ik dan toch te ver gegaan in FUD?

Mijn dochter is op zoek naar woonruimte in Amsterdam en omgeving. Die liggen niet voor het oprapen.
Zij staat dus in cyberland op verschillende plaatsen ingeschreven en volgt alle aanbiedingen die online staan.
Een paar maanden geleden ontdekte ze een leuke kamer in Amstelveen. Aan de buitenkant zag het er klein en oud uit, maar op de meegeleverde foto's oogde het binnen ruimer. Ze nam contact op met de verhuurster - die voor onbepaalde tijd naar Engeland was. Mijn dochter maakte een afspraak voor bezichtiging, verhuur, enz. De verhuurster gaf aan dat er meerdere kapers op de kust waren. Vandaar de vraag of mijn dochter een borgsom kon storten. Ook dat klinkt logisch - zeker als je de huizenmarkt in dit gebied kent.
Vervolgens kwam het verzoek de borg met Western Union over te maken, want de verhuurster had wat probleempjes met de bank. Toen rook mijn dochter meteen lont. En hoe graag ze ook woonruimte wilde, ze wist meteen dat dit niet zuiver was. Onderzoek leverde de ene leugen na de andere op. De advocaat die het contract had opgesteld bestond niet - een 'bounce' terug. De verhuurster bleek op LinkedIn te staan. Google-acties en gegevens uit haar mailwisseling lieten huurbare appartement in Genève en Zürich zien. De beschrijving van de inhoud, inclusief de foto's, waren gelijk aan die in Amstelveen… De verhuursite was heel bereidwillig om de listing te verwijderen. De trigger had gewerkt, dus ik had tóch genoeg FUD doorgegeven.

Hiermee zie je hoe de echte wereld en de cyberwereld verraderlijk dicht bij elkaar komen. Hoe weet je nog wat echt is? Nieuwe kanalen en malware vergroten dit probleem alleen maar. Mijn enthousiasme over de vele mogelijkheden om 'connected' te zijn, hebben mij nu ook bevreesd over mogelijke gevolgen. Hé wacht even, nu zit ik zelf met FUD…

INHOUDSOPGAVE

THE APPLICATION OF THE EPRIVACY DIRECTIVE ON RFID SYSTEMS

Dr. Eleni Kosta is a senior legal researcher at the Interdisciplinary Centre for Law & ICT (ICRI) – Institute for Broadband Technology (IBBT) of the K.U.Leuven, Belgium, and a part-time associate at the Brussels-based law firm time.lex. Eleni Kosta can be contacted at eleni.kosta@law.kuleuven.be

The emergence of RFID technology provides the potential for vast and varied applications, bringing with it both promise and peril. RFID tags used as the medium for the collection and transmission of personal data, as well as tracing devices for the location of natural persons open Pandora's Box regarding the privacy rights of the individuals. As many papers have been written on the protection of personal data of individuals in accordance with the Data Protection Directive, this paper focuses on the application of the ePrivacy Directive on RFID devices and systems.

Introduction

RFID technology has been known since the beginning of the previous century and was extensively used during the Second World War for the identification of airplanes as "friend or foe". Nevertheless it is considered as an emerging technology due to the fact that it enables a huge amount of innovative applications. RFID tags are not only used in manufacturing, logistics and the retail goods sector, but also in library cards, automotive sector, electronic passports, prisoner or patient armbands, to name just a few. RFID tags used as the medium for collecting and transmitting personal data, as well as tracing devices for the location of natural persons open Pandora's Box regarding the privacy rights of the individuals. Notwithstanding the positive impact of RFID technology in innovation, its deployment in several fields of everyday life poses severe threats to the privacy sphere of the individuals that do not know when, how and what kind of information about them is being transmitted at all times. In this paper we are going to briefly present some RFID applications and explain when they raise privacy concerns. We will then focus on the application of the ePrivacy Directive on them and will critically examine the recent amendment introduced to it in relation to data collection and identification devices.

RFID Applications and Privacy Implications

The use of RFID applications is increasing in the field of manufacturing and logistics, where they offer improved inventory control, increased labour efficiency, better customer services, etc. In these cases, however, it can be supported as a rule of thumb that no privacy issues arise, as there is no processing of personal data. Of course the landscape changes when the RFID tag can be associated with a natural person, such as the driver of the vehicle. If for instance an RFID tagged shipment inside a vehicle is linked to the identity of the driver and the RFID movement information is also used to monitor the employee's behaviour, checking amongst others the speed with which he is driving, then the data that relate to the RFID tag, reveal information about the driver and raise privacy concerns.

> The fact that an RFID tagged product can be connected to an individual, can allow for extensive profiling and raises privacy concerns

RFID technology is gradually expanding in different fields of everyday life, making it easy to collect personal information about the individuals and to track and trace them via products they carry or wear. In the consumer goods sector the bar codes are being gradually replaced by the Electronic Product Code (EPC), which is a unique number that identifies a specific item in the supply chain. Even if at first glance the introduction of the EPC might seem as not raising privacy issues, a second look will reveal otherwise. The fact that an RFID tagged product can be connected to an individual, for instance someone is carrying one, can allow for extensive profiling and raises privacy concerns. Libraries use RFID technology for tagging books and inlays but also into library cards, which allow the localisation of their owners. Hospitals use RFID technology to track the location of critical instruments and materials used inside body cavities during surgery, which may be left inadvertently. No privacy implications arise in the tagging of such surgical equipment. On the contrary the use of patient armbands and RFID tags that allow the localisation of the doctors and the nurses relate to the processing of personal data. RFID tags are also used as the storage medium for the European electronic passport [Kosta et al., 2007].

As a relatively recent trend it can be mentioned the use of RFID chips into the human body. Such implantation can take place for a variety of reasons. The Baja Beach Club in Barcelona offers RFID implants to the members of its VIP Club (Elliot, 2006). The RFID chip is implanted in the body of the VIP Members and gives them access to certain areas of the club and acts as a payment method at the bar. Tempting as it may sound, the RFID chip can be read by readers outside the Baja Beach Club and allows the tracking of the Club Members at any time.

The main characteristic of RFID tags in relation to privacy is that they are invisible and they facilitate the unnoticed collection of personal data. Such collection allows the localisation of the individuals at any time and thus their surveillance, revealing a lack of user control and transparency. The link between an RFID tagged product and an individual allows the development of profiling techniques and direct marketing is enabled when entering a specific area, while endangering consumer anonymity [Quirchmayr and Wills, 2007].

Applicability of the ePrivacy Directive

A lot has been written about the application of the Data Protection Directive to RFID applications. However, another complicated issue relates to the application of Directive 2002/58/EC (hereafter ePrivacy Directive) on RFID applications, which regulates specific issues regarding the processing of personal data in the electronic communications sector, and has triggered a vivid debate in the European Union. The ePrivacy Directive contains specific rules for the protection of privacy and the processing of personal data in the electronic communications sector, regulating issues such as confidentiality of communications, processing of traffic and location data and unsolicited communications. Aim of the ePrivacy directive is to protect the users of publicly available electronic communications services that are offered via public communications networks regardless of the technologies used, having as ultimate goal the achievement of technology neutrality (Rec. 4 ePrivacy Dir.). However, questions arise regarding the applicability of the ePrivacy directive to several emerging technologies, among which RFID [Cuipers et al, 2007].

Aim of the ePrivacy directive is to protect the users of publicly available electronic communications services

For the ePrivacy Directive to be applicable, three main questions should be answered to the affirmative:

1. whether there is an *electronic communications service*,
2. whether this service is offered in an *electronic* communications network and
3. whether the aforementioned service and network are *public*.

These terms are defined in article 2 (a, c, d) of the Framework Directive 2002/21/EC.

Emerging technologies, such as RFID, are usually transmission systems that permit the conveyance of signals in a wireless way [Cuipers et al, 2008, p. 884]. So, even if these networks differ from the traditional networks that the legislator had in mind at the time of the adoption of the electronic communications regulatory framework, they fall under the existing definition of electronic communications networks. [Cuipers et al, 2008, p. 891]. When the RFID application is part of a system that can be considered as a service, then they also qualify as an electronic communications service [Cuipers et al, 2008, p. 891]. More complicated is whether these networks and services fulfil the requirement of being 'public', which is a requirement for the application of the ePrivacy Directive.

The requirement for 'public' network and service

The term *public* in the context of electronic communications services and networks is not defined in the European framework for electronic communications. The lack of any

clear definition, as to when a network or a service should be in practice considered as public, has created a lot of difficulties not only in the interpretation of the relevant provisions of the framework, but also in the transposition of the Directives into the national legislations of the Member States. Significant problems arise especially in the context of new and emerging technologies that enable the deployment of new services and network, such as RFID.

The question of whether an electronic communications network or service is public does not seem to have a simple solution. There is lack of specific criteria on when an electronic communications service or an electronic communications networks is public in the legislation or in policy documents. In view of these *lacunae*, different and various criteria can be –and have already been– listed by different parties in order to define whether or not a network or service should be considered as public.

Such criteria could be quantitative, qualitative or a combination of both. For example, one could take into account whether the service or the network has been explicitly characterised as such by the relevant legislator, whether the service is offered by a provider whose primary activity is the provision of electronic communications services, whether it is the provider's intention to offer the service to anyone who requests it, whether the service or the network is aimed at a specific group of people, what is the breadth of the geographical area which is covered by the network or where the service is offered, whether standardised equipment is used etc [van der Hof et al, 2006, p. 152-153]. The multitude of criteria that can be used for the specification when a service or a network is public reveal the lack of consistent interpretation of the term throughout Europe. A clarification of the term at European level would contribute to the harmonised interpretation among the Member States and to the achievement of increased feeling of security to both citizens and the industry.

Public communications networks supporting data collection and identification devices

The scope of application of the ePrivacy Directive was modified via the Citizens' Rights Directive. The new Article 3 of the ePrivacy Directive stipulated that under public communications networks are included public communications networks that support data collection and identification devices:

Article 3 – Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, ***including public communications networks supporting data collection and identification devices.*** *(Emphasis added.)*

The amendment to Article 3 of the ePrivacy Directive was inspired by rigorous debates relating to RFID, which has been high on the agenda of the European Commission in the past few years. The Communication on RFID identified the situation that not all RFID applications are covered by the ePrivacy Directive [Commission of the European Communities, 2007, p. 5]. Taking this situation into account, the Commission wished to clarify that when RFID devices and applications are deployed in connection with public communications networks the ePrivacy Directive should also apply, in addition to the Data Protection Directive. The Directive clarified in Recital 56 that when such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of the ePrivacy Directive, including those on security, traffic and location data and on confidentiality, should apply.

The Communication on RFID identified the situation that not all RFID applications are covered by the ePrivacy Directive

It is questionable whether this addition to Article 3 of the ePrivacy Directive ('including public communications networks supporting data collection and identification devices') was therefore needed. The amendment that the Directive applies to public communications networks that support data collection and identification devices seems redundant, as the networks in question are public communications networks, which would anyway fall under the ePrivacy Directive.

More light on this debate is shed by Recital 56 which clarifies that when collection and identification devices "are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure", then the ePrivacy Directive is applicable. However the Recital makes reference to "electronic communications services" and not to publicly available electronic communications services. Article 3 is clear that only "publicly available electronic communications services" and not electronic communications services in general are covered by the ePrivacy Directive. Was the intention of the legislator to broaden the scope of application of the ePrivacy Directive to cover electronic communications services that are not publicly available when data collection and identification devices make use of such services? Unfortunately, it is not possible to give a definitive answer to this issue, based on the wording of either Article 3 or Recital 56.

Conclusion

The emergence of RFID technology provides the potential for vast and varied applications, bringing with it both promise and peril. Even if not every RFID application raises privacy threats, the fact that RFID tags are invisible and they facilitate the unnoticed collection of personal data has evoked great opposition from privacy activists and consumer protection organisations. The argument that honest citizens have nothing to fear, can easily be confronted by the counter-statement that a surveillance society, where RFID tags reveal personal information and enable the tracking and tracing of the individuals, shall be contested, as every law abiding citizens shall be free from any kind of monitoring (Flint, 2006).

The Citizen's Rights Directive wished to remove the confusion that existed in the past on whether the ePrivacy Directive applies to RFID applications by clarifying that public communications networks supporting data collection and identification devices fall under the scope of the Directive. Recital 56 was further introduced in order to assist in the better understanding of this amendment. Recital 56 should be read in conjunction with Article 3 of the ePrivacy Directive and be construed in a restrictive way. The interpreter of the law has to bear in mind that when the Recital refers to electronic communications services, it means publicly available electronic communications services, as only such services are, in principle, covered by the ePrivacy Directive. In any case, the added value of this amendment is not obvious. Was the addition "including public communications networks supporting data collection and identification devices" really needed? Does it mean that under the 2002 regime a public communications network that supported data collection and identification devices would not be covered by the ePrivacy Directive? To our opinion this was not the case. When a publicly available electronic communications service was offered over a public communications network, the ePrivacy Directive would apply, regardless of the fact whether this network was supporting data collection and identification devices or not. Therefore the addition "including public communications networks supporting data collection and identification devices" to Article 3 was not needed and does not offer any additional clarification to the scope of application of the ePrivacy Directive. In reality the new wording of Article 3 does not clarify any vague situations, nor offers additional legal clarity.

References

Commission of the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96 final, 15.03.2007

Cuijpers C., Roosendaal A. & Koops B.J. (ed.), "D11.5: The legal framework for location based services in Europe", FIDIS (Future of Identity in the Information Society) Project, 12 June 2007

Cuijpers, Colette and Koops, Bert-Jaap, "How fragmentation in European law undermines consumer protection: the case of location-based services" (2008) 33 European Law Review, p. 880-897.

Elliot V., "Speed through the check out with just a wave of your arm", The Times, 10 October 2006, available online at http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article666972.ece (last accessed 12 May 2007)

European Parliament and the Council of the European Union, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (23.11.1995).

European Parliament and the Counc il of het European Union, Directive 2002/12/EC of 7 March 2002 on a common regulatory framework for electronic Communications networks and services (Framework Directive) [2002] OJ L 108/33 (24.4.2002)

European Parliament and the Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (31.07.2002).

European Parliament and the Council of the European Union, Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Citizens' Rights Directive") [2009] OJ L337/11 (18.12.2009).

Kosta E., Meints M., Hansen M. & Gasson M., An analysis of security and privacy issues relating to RFID enabled ePassports, in IFIP International Federation for Information Processing, Volume 232, New approaches for Security, Privacy and Trust in Complex Environments, eds. Venter H., Eloff M., Labuschagne L., Eloff J. and Von Solms R., (Boston: Springer, 2007), pp. 467 – 472

Quirchmayr G. & Wills C. C., Data Protection and Privacy Laws in the Light of RFID and Emerging Technologies in C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.): TrustBus 2007, LNCS 4657, Springer Berlin / Heidelberg, 2007, pp.155-164

Van der Hof, Simone et al., Openbaarheid in het internettijdperk - De invloed van ICT op juridische concepten van openbaarheid (Sdu Uitgevers, Den Haag, 2006), p. 152-153.

Door Jeroen Aijtink, CISSP en Jan Wiersma, Int. Director EMEA DatacenterPulse.

EEN VIRUS IN JE NOODSTROOMGENERATOR

In de zomer van 2010 werd bekend dat er een zeer geavanceerd wormvirus was gevonden. Doel van dit wormvirus was de Iraanse ultracentrifuges te saboteren. Het virus was geprogrammeerd om programmacode in PLC's van Siemens te wijzigen en zo de motoren van de centrifuges te beïnvloeden. Het virus kreeg de naam Stuxnet mee, en kwam bekend te staan als het eerste virus dat industriële besturingssystemen als specifiek doel had.

Tot voor kort was het algemene idee dat SCADA- en industriële besturingssystemen kwetsbaar waren voor een cyberaanval voor velen slechts een theoretisch probleem. Door de grote complexiteit van deze systemen en hun bijzondere communicatieprotocollen waanden leveranciers en gebruikers zich veilig. De redenering erachter was dat complexe, industriële besturingssystemen zoals PLC's simpelweg zo verschillend zijn van normale IT-systemen dat deze geen interessant doel zijn voor 'traditionele' hackers. Meer bepaald zijn die verschillen:

- Industriële besturingssystemen bevatten componenten zoals PLC's, motor controllers en intelligente automaten, waarover de kennis van de gemiddelde hacker niet toereikend is;
- De componenten van die besturingssystemen zijn uitgevoerd in wijdvertakte netwerken met honderden onderdelen; alleen ervaren engineers begrijpen de complexiteit ervan;
- Ook de gebruikte communicatieprotocollen zoals Modbus en BACNet, zijn voor de meeste hackers onbekend. Datapakketten in dergelijke omgevingen zijn zonder specifieke kennis niet te vertalen;
- Zonder gedetailleerde kennis van de specifieke systeemarchitectuur zegt het merendeel van de systeemdata de hacker niet veel;
- Industriële besturingssystemen bevatten geen financiële of persoonlijke data - informatie die normaliter het doel is van een hacker.

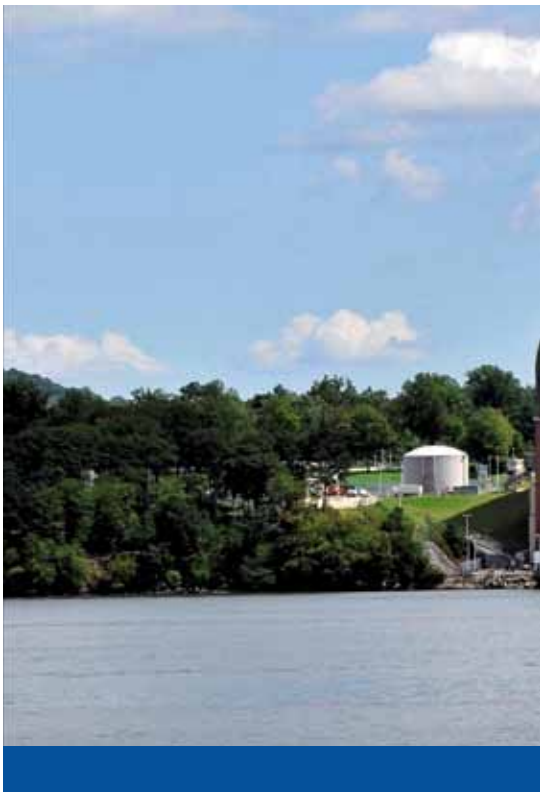
Een beveiligingsstrategie - als je het woord 'strategie' in deze context al kunt gebruiken - die puur is gebaseerd op systeemcomplexiteit en unieke systeemarchitecturen wordt door beveiligingsspecialisten ook wel 'security through obscurity' genoemd. Vaak zie je daarbij dat SCADA-netwerken slechts zijn beveiligd met een wachtwoord voor het bedienend personeel en niet veel meer.

> Stuxnet was het eerste virus met SCADA-systemen als doel

SCADA 2.0

In de afgelopen jaren is de wereld van industriële besturingssystemen en SCADA's echter behoorlijk veranderd. Oudere legacy-systemen bestonden nog uit speciale hardware, merkgebonden communicatieprotocollen en aparte communicatienetwerken. Moderne industriële besturingssystemen daarentegen bestaan uit standaard PC's en servers die communiceren via standaard IT-protocollen zoals IP, en delen hun netwerkomgeving met andere IT-eindgebruikernetwerken.
Deze verandering heeft diverse voordelen opgeleverd. Denk hierbij aan gereduceerde hardwarekosten en verhoogde flexibiliteit en bruikbaarheid.

Het bood de leveranciers van die industriële besturingssystemen bovendien de mogelijkheid om hun systeem te ontwikkelen op standaard Windows- of Unix-platformen. De systemen werden ook voorzien van 'features' om gemakkelijke data en rapportages te delen met andere IT- en netwerksystemen.
Gevolg hiervan is dat de grens tussen kantoorautomatiseringsomgevingen en de facilitaire industriële besturingssystemen in de afgelopen jaren vervaagde.

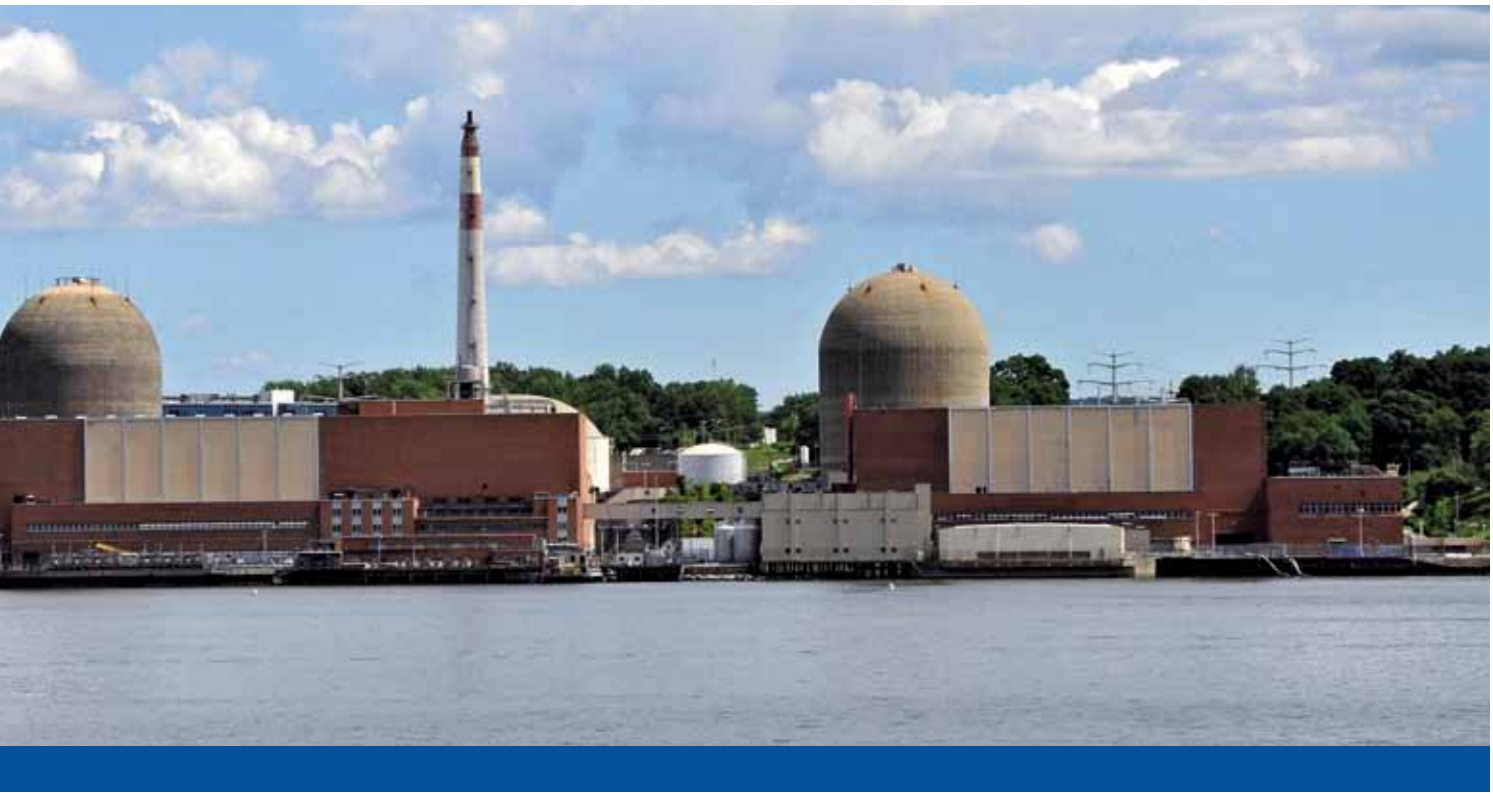


Dit had weer tot gevolg dat de nadelen van de traditionele IT-omgeving tastbaarder en groter werden, en met name de kans op 'cybercrime' toenam. In zijn 'Guide to Industrial Control System Security' waarschuwde het Amerikaanse National Institute of Standards and Technology (NIST) hier in 2008 al voor: "Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents."

> Moderne SCADA-systemen bestaan uit standaard computers die communiceren via standaard protocollen

Het instituut had zich hierbij onder meer gebaseerd op het onderzoek dat een team 'Department of Energy' (DOE) engineers van het Idaho National Engineering Lab in 2007 had uitgevoerd in het kader van het Aurora Project. Samen met hackers van het Department of Homeland Security (DHS) startten de engineers een cyber-aanval met als doel een grote dieselgenerator te vernielen. Enkele minuten nadat de hackers toegang hadden gekregen tot het SCADA-systeem, hadden ze de generator al onder controle. Op een video die in 2009 werd getoond in het Amerikaanse CBS-programma '60 Minutes' was te zien dat de 27 ton wegende generator werd gestart, flink begon te schudden en na enkele seconden volledig in rook gehuld was. De generator overleefde de cyber-aanval niet.
Dit Aurora Project toonde daarmee aan dat het voor hackers mogelijk was via een netwerktoegang fysieke schade toe te brengen aan een generator. De hackers hadden hierbij kwetsbaarheden gebruikt die vandaag de dag in de meeste industriële besturingssystemen aanwezig zijn.

Beveiligen van een SCADA-netwerk
Maar zoals zo vaak heeft elk nadeel zijn voordeel. Het feit dat leveranciers van moderne SCADA-systemen deze hebben gebaseerd op standaard IT-onderdelen en -protocollen, heeft logischerwijs ook als voordeel dat er al veel kennis is over de beveiliging van dergelijke omgevingen.
Net als in de 'echte IT-wereld' begint een goed beveiligde omgeving bij het bepalen van de bedreigingen en risico's voor de organisatie en haar infrastructuur. Als de facilitaire systemen worden gecombineerd met de IT-omgeving is de stelling "we hebben toch een firewall" niet meer afdoende. Wat nodig is, is goed ontworpen zonering, zodat de buitenwereld - en ook de datastromen voor kantoorautomatisering - en de facilitaire systemen van elkaar zijn gescheiden met eigen zones. Hier hoort ook inspectie van de communicatiestromen bij met behulp van 'intrusion detection-systemen'.
Naast beveiligingsmaatregelen binnen een netwerk is het van belang servers, besturingssystemen, applicaties en databases goed te beveiligen en te voorzien van de laatste 'patches' en antivirussoftware. Niet alleen na installatie, maar in een doorlopend proces.
Tot zover de beveiliging die een organisatie zelf helemaal in de hand kan houden. Maar steeds meer facilitaire systemen hebben ook remote-support vanuit de leverancier. Het is hierbij zaak goed na te denken over welke informatie de organisatie mag verlaten. Daarnaast is het de overweging waard de leverancier alleen toegang te geven wanneer er daadwerkelijk een probleem ís. Het oplossen van storin-



gen vanuit de locatie lijkt ouderwets, maar geeft wel de meeste controle. Zeker wanneer de monteur wordt begeleid door iemand die inhoudelijk kan beoordelen wat hij uitvoert. Bovenstaande lijkt af te wijken van de visie van het Jericho Forum. Jericho gaat uit dat netwerken strikt genomen zonder 'firewall-slotgrachten' kunnen. Dit vanuit de overtuiging dat beveiliging wordt aangebracht daar waar dat nodig is op de servers en werkplekken. De traditionele firewall zou hierdoor overbodig worden. Wanneer de beveiliging op alle systemen integraal is geregeld, kan de firewall helemaal uit. Maar voordat dit moment is aangebroken voor SCADA-systemen, hebben veel organisaties en leveranciers nog een lange weg te gaan.

Kort over Jeroen Aijtink
Jeroen Aijtink is senior ontwerper bij de overheid. Hij houdt zich bezig met het ontwerpen van netwerkbeveiliging en veilige koppelingen naar externe netwerken. Aijtink is opgeleid in de Informatie- en Communicatietechnologie en heeft naast zijn CISSP-certificering veel detailkennis van security componenten.

Kort over Jan Wiersma
Jan Wiersma is technisch manager bij EvoSwitch, een toonaangevend, hypermodern datacenter in de regio Amsterdam dat geheel CO2 neutraal opereert. Wiersma is opgeleid in zowel de Informatie- en Communicatietechnologie als in de proces- en milieutechnologie. Hij vertegenwoordigt EvoSwitch in diverse nationale en internationale normencommissies zoals de ASHRAE (TC9.9), Open Datacenter Alliance (ODCA) en NEN (NC381888). Jan Wiersma is ook de internationale directeur EMEA voor DatacenterPulse, het platform voor eindgebruikers en exploitanten van datacenters. Jan is te bereiken via j.wiersma@evoswitch.com

> De generator werd gestart, begon te schudden en was na enkele seconden gehuld in rook

Stuxnet
In de lente van 2010 ontdekte de beveiligingsfirma VirusBlokAda een virus dat was geschreven om kwetsbaarheden in industriële besturingssystemen te exploiteren. Men vond een stuk malware in het industriële besturingssysteem van een Iraanse klant, verborgen in de programmacode dat de naam Stuxnet kreeg. Een analyse van Stuxnet door de beveiligingsfirma Symantec bracht aan het licht dat het een computerworm betrof die de mogelijkheid had om zich zelf van PC naar PC te verplaatsen en zich te vermenigvuldigen zonder menselijke interventie. Stuxnet heeft zelfs de mogelijkheid zich te verspreiden zonder een netwerkconnectie. Het analysedossier van Symantec beschrijft de worm als "een van de meest complexe die men ooit heeft geanalyseerd".

De complexiteit en het raffinement van het Stuxnet-virus maakte het al bijzonder, echter het doel van het virus maakt het echt uniek. Daar waar traditionele malware IT-systemen als doel had, was Stuxnet specifiek geschreven voor het aanvallen van industriële besturings- en SCADA-systemen. De worm vermenigvuldigde zichzelf via het internet van PC naar PC tot deze uiteindelijk via de PC, laptop of zelfs USB-disk van een nietsvermoedende onderhoudstechnicus toegang kreeg tot de juiste faciliteit. Zodra Stuxnet het juiste systeem kon infecteren, opende het virus een 'back door' waardoor ongeautoriseerde personen toegang kregen tot het facilitaire systeem. Op deze manier kon men gegevens van de lay-out en parameters van het SCADA-systeem downloaden. Daarnaast kon Stuxnet ongemerkt programmacode van PLC's herschrijven die onderdeel waren van de communicatie in het industriële besturingssysteem. Alle intelligentie voor deze actie was onderdeel van Stuxnet, en daarbij was geen externe toegang of hulp nodig. Op deze manier kon men de controle van het industriële besturingssysteem ongemerkt overnemen en enorme schade aanrichten in een bedrijfskritische omgeving.

HACKEN IS GEEN OPSPORINGSBEVOEGDHEID!

Jan-Jaap Oerlemans

Mr. J.J. Oerlemans is promovendus bij de afdeling eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij van de Universiteit Leiden en daarnaast juridisch adviseur bij het IT beveiligingsbedrijf Fox-IT. Hij doet onderzoek naar digitale opsporingsmethoden en jurisdictie op internet.

Het hacken van een persoonlijke computer om bewijsmateriaal te verzamelen van een verdachte, steunt op geen enkele wettelijke grondslag. Die wettelijke grondslag is echter wel vereist op grond van het strafvorderlijk legaliteitsbeginsel en vloeit tevens voort uit de vereisten van het Europese grondrecht op privacy, zoals vastgelegd in artikel 8 van het Europees Verdrag van de Rechten van de Mens. Het (te) ruim interpreteren van bestaande opsporingsbevoegdheden is niet wenselijk en nagegaan moet worden welke nieuwe bevoegdheden eventueel noodzakelijk zijn om misdaad effectief te blijven bestrijden.

Waarborgen vertrouwelijkheid

Toch lijken de politie en justitie op de feiten vooruit te lopen. Er zijn op zijn minst aanwijzingen dat de opsporingsmethode in de praktijk al incidenteel wordt toegepast. Zo bleek eind oktober 2011 bijvoorbeeld dat een Duits bedrijf spionagesoftware aan Nederlandse autoriteiten heeft geleverd. Onduidelijk is of de software ook door de Nederlandse politie wordt gebruikt. Het plaatsen van spionagesoftware op een computer van een verdachte vergt ofwel het 'fysiek' inbreken op een computer van de verdachte tijdens een huiszoeking, ofwel digitaal inbreken - op afstand via internet - waarbij de software op een computer wordt geplaatst. In dit laatste geval is daar voor de politie en justitie een grondslag in de wet voor vereist. Die wettelijke grondslag is vereist, omdat hacken op een persoonlijke computer een ernstige inbreuk op de persoonlijke levenssfeer van de betrokkene levert. Mensen gaan er van uit dat de integriteit en vertrouwelijkheid van hun computer zijn gewaarborgd. En dat de overheid niet zo maar in hun computer mag rondkijken of communicatie kan afluisteren.

> Die wettelijke grondslag is vereist, omdat hacken op een pc een ernstige inbreuk oplevert

Inkijkoperatie

De redenatie dat hacken onder de bijzondere opsporingsbevoegdheid van een 'inkijkoperatie' valt, is een te grote oprekking van de opsporingsbevoegdheid. Een inkijkoperatie mag namelijk alleen worden uitgevoerd in een 'besloten plaats' en daarmee wordt juridisch gezien iets anders bedoelt dan een computer, bijvoorbeeld een woning, garage of loods. Bovendien is de privacy-inbreuk bij het inbreken op computers anders dan die bij fysieke plaatsen. Het gaat ook te ver de bijzondere opsporingsbevoegdheid van 'direct afluisteren' gelijk te stellen aan het hacken van een computer waarbij zelfs in een computer kan worden rondgekeken. De privacyinbreuk bij hacken ziet ook toe op andere aspecten van de persoonlijke levenssfeer - naast het afluisteren van vertrouwelijke communicatie. Met de bevoegdheid van direct afluisteren werd oorspronkelijk overigens iets heel anders bedoeld. Het mogelijk maken van het plaatsen van spionagesoftware op afstand en andere vormen van hacken moet ook noodzakelijk zijn. Anonimiteit en versleuteling op internet vormen be-

> Anonimiteit en versleuteling vormen belangrijke argumenten voor het mogelijk maken van hacken

langrijke argumenten voor het mogelijk maken van hacken door de politie en justitie. In digitale opsporingsonderzoeken zijn verdachten vaak alleen identificeerbaar via hun IP-adres en dat IP-adres kan via allerlei technieken worden afgeschermd. Door een computer waarvan de verdachte gebruik maakt te hacken kan het werkelijke IP-adres van de computer worden achterhaald.

Waarvoor is de overheid verantwoordelijk?

Zelfs als het ware IP-adres van de computer van de verdachte bekend is, kan het vergaren van bewijsmateriaal via een doorzoeking, inbeslagneming of telecommunicatietap worden belemmerd door gebruik van versleuteling. Versleuteling kan zowel zien op het afschermen van communicatie via internet als op het onleesbaar maken van data op gegevensdragers. Met spionagesoftware kan communicatie bij de bron worden afgetapt waardoor het probleem van versleuteling kan worden omzeild. Daarnaast kunnen toetsaanslagen en daarmee ook het wachtwoord dat voor versleuteling van gegevensdragers wordt gebruikt, worden onderschept. Op deze manier kunnen de effecten van versleuteling ongedaan worden gemaakt.

Het opheffen van anonimiteit en ongedaan maken van versleuteling zijn de belangrijkste argumenten voor het mogelijk maken van bepaalde vormen van hacken als opsporingsbevoegdheid. In plaats van bestaande bevoegdheden op te rekken, waardoor de grenzen van de bevoegdheden onduidelijk worden, moeten ingrijpende nieuwe opsporingsmethoden door de wetgever duidelijk worden genormeerd. Natuurlijk op voorwaarde dat de nieuwe opsporingsbevoegdheden door het parlement noodzakelijk worden geacht. Naar mijn mening is die noodzaak aanwezig.

> Na de IRT-affaire hebben wij ervoor gekozen opsporingsmethoden die een ernstige inbreuk op privacy maken expliciet vast te leggen in de wet

Na de IRT-affaire hebben wij er als maatschappij voor gekozen opsporingsmethoden die een ernstige inbreuk op privacy maken expliciet vast te leggen in de wet. Op die manier weten zowel opsporingsambtenaren als de betrokken burgers waar zij aan toe zijn en worden de risico's op misbruik van opsporingsmethoden geminimaliseerd. Keerzijde van ons systeem is dat deze regelmatig moet worden aangepast aan nieuwe ontwikkelingen in de maatschappij. Hierbij moeten verregaande opsporingsmethoden in de wet worden vastgelegd. Het is nu aan de wetgever haar verantwoordelijkheid daarvoor te nemen.

COLUMN

HET RECHT OM JE JEUGDZONDEN TE LATEN WISSEN

Onlangs is het Europese wetsvoorstel voor vernieuwing van onze privacywetgeving uitgelekt. Een van de belangrijke punten in het voorstel is 'The right to be forgotten'. Over dit recht om vergeten te worden, is in academische kringen een aspect van privacy waarover al enige jaren een verwoede discussie wordt gevoerd. Want enerzijds constateren wetenschappers dat het internet een eeuwig geheugen heeft en dat dit de privacy van personen niet ten goede komt. Anderzijds betwijfelen zij of je ook echt effectief iets aan die eeuwigheidswaarde van het internet kunt doen. Over hoe dat recht vormgegeven moet worden, bestaan nog steeds heftige discussies. De Europese wetgever heeft het in ieder geval zo'n groot probleem gevonden dat het belangrijk is dat er een recht gecreëerd moet worden.
In het voorstel staat:
"The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data […]".
In vier gevallen kan een datasubtject (lees: een persoon van wie gegevens worden verwerkt) een beroep doen op deze bepaling.

1. Als de gegevens niet langer noodzakelijk zijn voor het verwezenlijken van het doel waarvoor ze werden verzameld;
2. Als de persoon om wiens gegevens het gaat zijn toestemming intrekt of als de maximum bewaartermijn is verstreken;
3. Als er door de persoon wiens gegevens worden verwerkt bezwaar is gemaakt tegen het verwerken;
4. Als de verwerking van de persoonsgegevens anderszins in strijd is met deze regeling.

Het is een zeer uitgebreide bepaling waarin heel veel punten voor discussie staan. Ik behandel die hier niet, omdat ik dan waarschijnlijk een paar pagina's verder ben. Maar wat volgens mij erg belangrijk is, is dat jongeren heel specifieke aandacht krijgen. De wetgever heeft daarover de volgende zinsnede opgenomen in de voorgestelde bepaling: "This right shall apply especially in relation to personal data which are made available by the data subject while he or she was a child." De wetgever *hoeft* dit niet expliciet op te nemen omdat de reikwijdte ruim genoeg is en alle datasubjecten omvat. Dat zij dit toch heeft gedaan, geeft aan hoe belangrijk zij het vindt dat jongeren in de online wereld van alledag worden beschermd tegen onder meer zichzelf. Het gaat immers om persoonlijke informatie die zij zelf online hebben gezet toen zij nog kind waren. De wetgever geeft in de uitleg bij deze bepaling aan dat dit recht voor het verwijderen van 'jeugdzondes' vooral relevant is, omdat jongeren zich mogelijk nog niet volledig bewust zijn van de risico's die zijn verbonden aan het online plaatsen van informatie. Dit is volgens mij een zeer belangrijke constatering die ik van harte onderschrijf. In mijn lezingen probeer ik vaak aan te geven dat jongeren letterlijk nog niet volwassen zijn en dat hun hersens ook nog niet zijn volgroeid. Een belangrijk gevolg daarvan is dat zij heel anders met risico's omgaan dan volwassenen. Sterker nog: zij zien vaak geen risico's - daar waar volwassenen deze zonder moeite kunnen benoemen. Ik zie helaas nog wel twee gaatjes in deze - verder mooie - bepaling. Wat te doen als een ander informatie over jou plaatst? Jongeren (en ook volwassenen) zetten vaak persoonlijke informatie online die ook anderen raakt. Denk aan die foto of dat filmpje dat werd gemaakt van een jongere terwijl hij/zij dronken was en 'door een vriend' op Facebook is gezet. Mogelijk kun je dan een beroep doen op grond 3 of 4, maar of dit in de praktijk ook echt werkbaar of mogelijk zal zijn, durf ik (nu nog) niet te zeggen. Een tweede, wat kleiner bezwaar, heeft te maken met volwassen zondes. Ik kom online heel vaak informatie tegen die door (jong)volwassenen zijn geplaatst die ook echt het verwijderen waard is. Jongeren zijn namelijk zeker niet de enigen die jeugdige zondes begaan. Zij zouden de toestemming kunnen intrekken, wat zoals gezegd ook een grond kan zijn voor het inroepen van dit recht om vergeten te worden. En wellicht is het ook wel zo eenvoudig dat van volwassenen meer verwacht mag worden in de zelfbescherming. Dat het daar toch nog regelmatig fout gaat, mag daar niet aan afdoen. Maar juist omdat ik zie dat het daar toch nog vaak misgaat, lijkt me wel dat we naast deze nieuwe voorgestelde wetgeving nog een hele andere grote taak hebben: bewustwordingsvergroting bij alle gebruikers in de online wereld. Dat zou wat mij betreft heel hoog op de agenda mogen staan.

mr Rachel Marbus
@RachelMarbus op Twitter

EXPLOSIEVE GROEI VAN ANDROID MALWARE

Jeroen Willemsen is een expert mobiele technologie en security consultant bij Domus Technica.
Hij is te bereiken via jeroen.willemsen@domustechnica.com.

Er is steeds meer aandacht voor malware op het Android platform. Op basis van verschillende onderzoeken maken partijen hun metingen en onderzoeken openbaar over hoe het met de veiligheid van Android is gesteld.

Allereerst zijn er 'security vendors' zoals Juniper, McAfee, Bit9 en Lookout Mobile Security. Zij waarschuwden al voor de illegale apps die in alternatieve app-markets verschenen in onder meer China en Rusland. Onder deze illegale apps bevinden zich zowel gekraakte betaalde apps als aangepaste gratis apps. In beide gevallen is er een verhoogde kans dat deze apps malware met zich meedragen. Ook hebben verschillende security vendors regelmatig gerapporteerd over nieuwe malware samples. Over precieze aantallen en over de totale groei zijn er verschillende cijfers bekend. Zo laat de infographic van het Juniper Global Threat Center[1] een stijging van 472% zien van het aantal malware samples tussen juli 2011 en 10 november 2011. McAfee komt met wat voorzichtigere cijfers in zijn kwartaalrapport, maar ook daar is de groei duidelijk aanwezig.

Naast de gerapporteerde malwaregroei, blijkt dat producenten hun Android-smartphones niet blijven updaten. Een opvallend rapport over dit feit komt van Bit9. Zij kwamen met de 'dirty dozen list': een lijst van twaalf smartphones die erg populair zijn, maar die niet worden voorzien van de laatste updates[2]. Daarnaast waarschuwden verschillende onderzoekers over de mate waarin Android-toestellen zijn beveiligd. De resultaten laten rapportages zien over nieuw ontdekte malware, over het feit dat apps van de fabrikanten permissies lekken en over aanvallen van buffer overflow die root-access kunnen geven.

Deze aandacht is op zich niet verkeerd: Android is namelijk een platform wat nog hard aan het groeien is, en met die groei natuurlijk ook meer malwareschrijvers aantrekt. Want hoe groter de doelgroep, hoe meer potentiële winst er aanwezig is voor een malwareschrijver. De vraag is alleen of er met deze getallen geen onnodige paniek kan uitbreken.

> Producenten updaten hun Android smartphones niet lang

Niet alleen aandacht, ook actie

Google heeft zeker niet stil gezeten: er zijn meerdere updates vrijgegeven voor het mobiele besturingssysteem. Ook heeft Google tot nu toe alle apps waar malware in werd gevonden, binnen korte tijd verwijderd uit de Market, zoals bijvoorbeeld de apps die DroidDream light malware en de apps met Plankton malware.

Zeker meer malware, maar geen epidemie: getallen in een beter perspectief

Het klopt inderdaad dat er meer malware is verschenen, ook binnen de Android Market. Maar veel van de malware waarover wordt gerapporteerd, bevindt zich in de eerdergenoemde alternatieve app-markets. Een gebruiker die zijn apps uit een enterprise market of uit de Android Market haalt, heeft daar minder last van. Daarnaast is het aantal geïnfecteerde apps binnen de Android Market bijzonder laag. Het is erg moeilijk om de precieze statistieken

Malware apps die de Market haalden

Twee van de meest bekende malware samples die in de Android Market opdoken zijn Plankton en DroidDream:

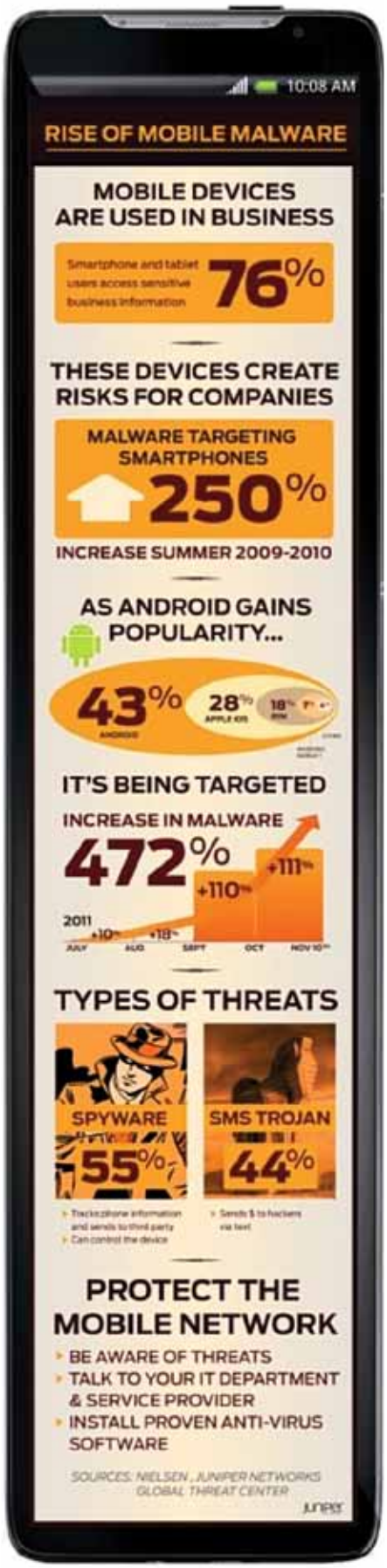
Plankton

Plankton[3]: een sample die in juni 2011 is gevonden, in apps zit verpakt als backgroundservice en op commando code kan uitvoeren van een server. Plankton heeft ook een verwant, YZHCSMS[4], die smsjes naar een premium nummer verstuurd.

DroidDream

Een ander malware sample dat eind 2010 is gevonden, is DroidDream[5]. Dit sample maakt gebruik van zwakheden in het Android platform van Android versie 2.2.1 en lager. De malware krijgt roottoegang en kan nieuwe code laden. Een broertje van DroidDream is DroidDream Light (DDLight)[6].

te verkrijgen, maar het lijkt erop dat het aantal is gegroeid van 29 met malware geïnfecteerde apps in de zomer van 2010 naar ± 100-150 aan het einde van 2011. Dan lijkt 472% [1] opeens niet meer zo'n eng getal, zeker omdat er meer dan 370.000 Android apps zijn. Dat betekent dat minder dan 0.04% van de apps op dit moment gedetecteerde malware bezit.



Illustratie 1 - De groei van mobiele malware (bron: Juniper Global Threat Center)

De media en de security-vendors blazen de hoeveelheid malware wel op

Hoe reëel is de dreiging?

Hoewel er wel een groei is in de hoeveelheid malware op het Android platform, is de kans dat een eindgebruiker hiermee in contact komt van een aantal factoren afhankelijk.

Een gebruiker die bijvoorbeeld alternatieve app-markets gebruikt, of illegale versies van apps downloadt, of twijfelachtige websites en/of apps gebruikt heeft zeker een verhoogd risico op het binnenhalen van malware. Daarnaast verhogen activiteiten zoals het gebruiken van een Custom rom, het rooten van de smartphone en het gebruik van een sterk verouderde versie van het Android platform het risico.

Natuurlijk: als een gebruiker zich aan deze regels houdt, bestaat de kans in aanraking te komen met malware nog steeds. Daarom kunnen gebruikers het beste:

- Alleen apps installeren van developers en app-markets die je vertrouwt, zoals de Google Android Market of de Amazon App store.
- De permissies logisch beoordelen. Hoort deze app toegang te hebben tot de contacten? Tot de locatie-informatie? Of tot de telefoonstatus?
- Nadenken bij het rooten van het apparaat en het installeren van Custom

Custom roms en rooten

Het gebruik van Custom roms en het rooten van een smartphone is niet hetzelfde. Custom roms zijn Rom-versies voor een apparaat die zijn gemaakt door andere partijen dan de standaardleverancier van de hard-/software. Een goed voorbeeld is de Cyanogenmod rom. Deze rom wordt geïnstalleerd met een aangepaste recovery. Om die te verkrijgen dient men vaak root-/Super User-toegang tot het toestel te verkrijgen. Het verkrijgen van deze toegang heet rooten. Het rooten van een toestel kan ook andere doeleinden hebben dan het kunnen installeren van Custom roms. Voorbeelden van andere motivaties om root-/Super User-toegang te krijgen, zijn onder meer: het de-installeren van apps die de telefoonleverancier erop heeft gezet en het kunnen gebruiken van bepaalde apps die zonder root/Super User-toegang niet kunnen functioneren.

Illegale apps

Illegale apps presenteren zich als een originele app, maar zijn dat niet! Ze komen bijvoorbeeld van een andere leverancier, die een functionaliteit heeft veranderd of malware heeft toegevoegd. Kijk dus goed naar wie de app heeft uitgegeven. Inventariseer of er online al eerder over gerapporteerd is, of de originele producent naar hetzelfde product linkt en of de download-statistieken kloppen. Ook kan het zo zijn dat de legale app gratis is en de illegale versie geld kost. Een voorbeeld is een gekraakte versie van de betaalde versie van het bekende spel 'Fruit Ninja'. Dit is te downloaden via apkcute.com.

Let wel: binnen dit artikel gebruiken we steevast het woord 'illegaal'. Echter, het gebruik van de naam van een app en/of merk en/of kleuren is niet in alle landen strafbaar. Daarom zou het woord 'malafide' wellicht beter de lading dekken.

roms. Wegen de risico's op tegen de meerwaarde?
- Nadenken over wat wel en wat niet op te slaan op een smartphone. Gevoelige bedrijfsinformatie en wachtwoorden kun je bijvoorbeeld beter niet onbeveiligd opslaan.
- Op internet kijken of de apps ook echt veilig zijn, én of ze ook een goede naam hebben.
- Een effectieve mobiele virusscanner installeren, zoals F-secure of Kaspersky.
- Contact opnemen met de developer als je erg twijfelt. Gebruik dit als allerlaatste redmiddel: dus alleen als je erg twijfelt. Via de Market kun je contact opnemen met de betreffende developer.

Maar wiens verantwoordelijkheid is het nu?

Het begint bij Google. In tegenstelling tot Apple geeft Google de gebruikers erg veel vrijheid. Dat geldt zowel voor het publiceren van apps via de Android Market als bij het installeren van apps via alternatieve bronnen. Eén van de maatregelen die Google zou kunnen nemen, is bijvoorbeeld een strenger publicatiebeleid. Zo zijn er al regels waar een app aan moet voldoen. Helaas worden apps hierop niet gecontroleerd voordat ze gepubliceerd zijn.

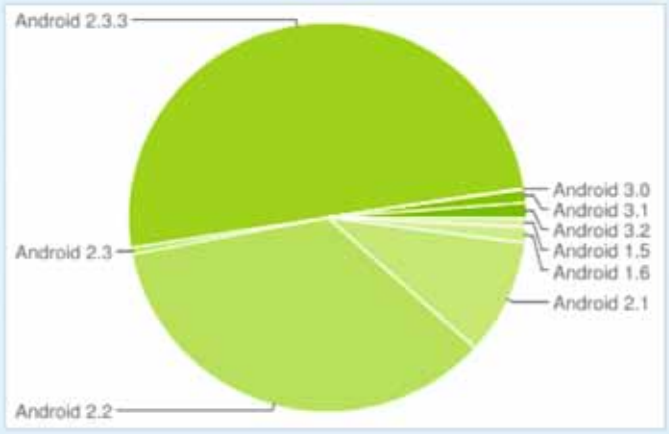
Een andere maatregel ligt meer bij de leveranciers van toestellen: zij dienen hun toestellen vaker te updaten, zeker als het gaat om het uitrollen van security patches. Dit gaat echter niet zonder slag of stoot, omdat de updates ook door de telecomproviders moeten worden getest. De toestellen moeten namelijk na de update ook nog gewoon werken en geen operator-specifieke regels en afspraken overtreden. Daarom dienen Google, de eerder genoemde security vendors, de telecomproviders en de smartphoneleveranciers de handen ineen te slaan om de security-patch cyclus te versnellen. Er ligt echter al direct een uitdaging bij deze maatregel: smartphone leveranciers verdienen geld door het leveren van nieuwe toestellen en niet door het leveren van software-updates. Dit verdienmodel motiveert de huidige leveranciers dan ook niet om hardware lang te blijven ondersteunen.

> Google kan een strenger app-publicatie beleid aannemen

> De gebruiker dient wel zelf actief na te denken

Om dit te ondervangen wil Google het aantal major updates verkleinen naar één update per jaar, zodat developers daar optimaal gebruik van kunnen maken. Maar daarmee is het nog niet zeker dat alle security issues tijdig worden ondervangen. Hiervoor kan Google wellicht afspraken maken met de smartphoneleveranciers. Een andere optie is het gebruiken van meer gestandaardiseerde hardware, zodat het goedkoper wordt om security patches voor de verschillende toestellen uit te rollen. Dit limiteert alleen wel het aanbod en de vrijheid van de smartphoneleveranciers. Het gebruik van betaalde updates kan een ontwikkelaar motiveren, maar dit kan problemen veroorzaken door het huidige licentiemodel rondom Android.

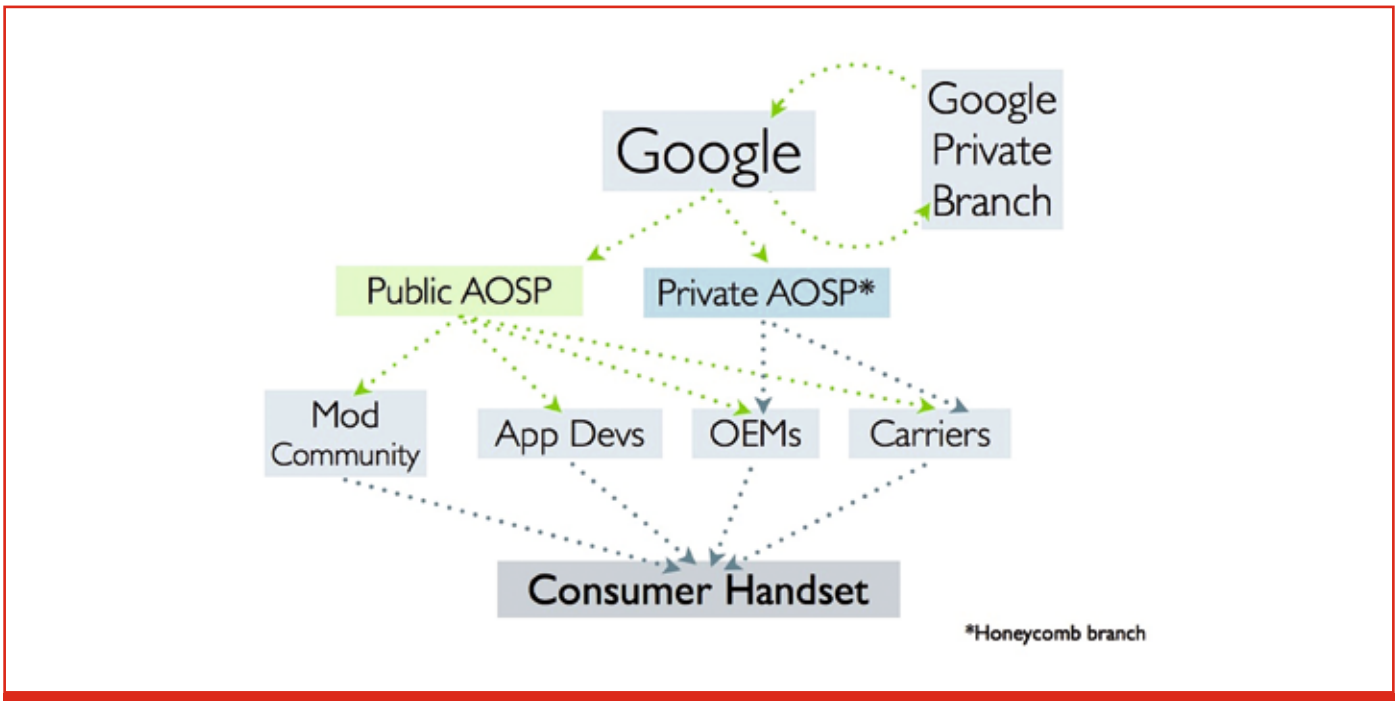
Hoewel uit het bovenstaande is op te maken dat Google en de smartphoneleveranciers voor een deel verantwoordelijk zijn, ligt de uiteindelijke verantwoordelijkheid toch voor een groot deel bij de gebruiker. Naast de bovengenoemde maatregelen dient de gebruiker zelf actief na te denken welke smartphone hij kiest, wat hij er vervolgens doet en welke risico's er aan



Platform	Codename	API Level	Distribution
Android 1.5	Cupcake	3	0.8%
Android 1.6	Donut	4	1.3%
Android 2.1	Eclair	7	9.6%
Android 2.2	Froyo	8	35.3%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	50.1%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.1%
Android 3.2		13	1.2%

Data collected during a 14-day period ending on December 1, 2011

Illustratie 2 - De huidige verspreiding van Android-varianten (bron: developer.android.com)



Illustratie 3 - Android source updatepaden (bron: Lookout.com)

die acties kleven. Het is dus ook van belang dat de gebruiker op een eerlijke manier wordt voorgelicht.
Natuurlijk wordt dit wat complexer bij het gebruik van enterprise-informatie en bij het toestaan van gebruikers-eigen apparaten binnen de enterprise (de bring-your-own-device trend).
Dan is het verstandig om de verantwoordelijkheden van de beheerder en de gebruiker formeel goed vast te leggen en aanvullende maatregelen te nemen, voor zover dat wettelijk is toegestaan en technisch mogelijk is. Maatregelen zijn dan bijvoorbeeld: het gebruik van eigen enterprise app-markets, mobile device management oplossingen en virtualisatie-oplossingen.

Conclusie

Ja, er is zeker een stijging in de hoeveelheid malware op toestellen van Android. Echter: de media en de security vendors blazen dat op dit moment wel op. Het is absoluut verstandig om kritisch te blijven kijken naar het Android-platform, omdat er door de groei van het aantal gebruikers ook een grotere potentie in het platform schuilt voor malwareschrijvers. Daarnaast zorgen de huidige staat van de Android Market en de manier waarop smartphoneleveranciers omgaan met het geven van toestel-updates, wel voor een verhoogd risico op malware. Daarom kan het ook goed zijn dat security vendors deze aandacht/hype creëren. Maar uitsluitend als dit ook daadwerkelijk leidt tot het verbeteren van de situatie.
Hoe dan ook: een groot deel van het risico op malware-infecties zit in het gedrag van de gebruiker zelf. Als de gebruiker twijfelachtige of illegale apps wil blijven gebruiken, is de kans op een malware-infectie zeker groot. Datzelfde geldt uiteraard voor alternatieve app-stores en twijfelachtige websites.

Referenties

[1] *Blog-entry op Juniper Global Threat Center 'Mobile Malware Development Continues To Rise, Android Leads The Way' d.d. 15 November 2011: http://globalthreatcenter.com/?p=2492*

[2] *BIT9 REPORT 'The Most Vulnerable Smartphones of 2011' d.d. 21 November 2011: http://www.bit9.com/files/Bit9Report_SmartPhones2011.pdf*

[3] *Plankton: http://www.csc.ncsu.edu/faculty/jiang/Plankton/*

[4] *YZHCSMS: http://www.csc.ncsu.edu/faculty/jiang/YZHCSMS/*

[5] *DroidDream: http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/*

[6] *DroidDream Light: http://blog.mylookout.com/2011/05/security-alert-droiddreamlight-new-malware-from-the-developers-of-droiddream/*

Herman van Rongen is Consultant Business Continuity & Account Delivery Manager voor HP Continuity Services.
Rob van Ewijck is Sales Executive, en daarmee commercieel verantwoordelijk voor HP Continuity Services.

HOEVEEL CONTINUÏTEIT WIL JE HEBBEN...?

Business en IT communiceren vaak niet goed met elkaar. De gebruiker verwacht altijd dat alles werkt. Maar IT heeft per definitie een tekort aan budget om dat te kunnen garanderen. Als beiden weten wat de ander wil, scheelt dat in kosten, verkeerde verwachtingen en frustratie.

IT-afdelingen willen hun zaken graag goed voor elkaar hebben; zij willen IT continuïteit leveren. De business eist dit in eerste instantie vaak ook: 'het moet gewoon werken' en 'dataverlies is onacceptabel'. Zijn deze eisen goed onderbouwd en zijn de kosten die daarmee gepaard gaan echt nodig? Waarom investeert men überhaupt in continuïteitsmaatregelen? Investeringen die alleen op gevoel zijn gebaseerd, zijn vaak niet de allerbeste.

Zowel de business als het management of de ondernemer zullen niet alleen moeten aangeven wat ze van IT verwachten, maar ook tegen welke kosten. Dat vraagt om duidelijke afspraken waarin bijvoorbeeld is vastgelegd hoe goed IT zijn continuïteit moet hebben geregeld en binnen hoeveel tijd feitelijke 'service' wordt geleverd. Dit gaat uiteraard ook op in onvoorziene situaties...

Een Business Impact Analyse (BIA) is de geëigende methode om deze discussie tussen IT en Business op gang te brengen. Bovendien is deze methode geschikt om te bepalen wat geschikte continuïteitsmaatregelen zijn.

'...het moet gewoon werken'

Business Impact Analyse

Bij een Business Impact Analyse (BIA) wordt het volgende bepaald: hoe ernstig is het als over bepaalde bedrijfsprocessen niet beschikt kan worden? Hierbij wordt zowel voor- als achteruit in de tijd gekeken (seconden, minuten, uren, dagen en weken). Het vooruitkijken levert een indicatie op. Hoelang kunt u na een calamiteit zonder een bedrijfsproces overleven? Dit wordt aangeduid met *Recovery Time Objective* (RTO). Het achteruitkijken levert het moment waarop de laatste vitale gegevens veiliggesteld moeten zijn, aangeduid met de term *Recovery Point Objective* (RPO). Hoe lang u zonder uw bedrijfsproces kunt, betekent vaak: hoe lang kunt u zonder IT?
Voor managers is een middenweg nooit een optie. Intuïtief zeggen ze meestal dat het bedrijf nog geen minuut zonder alle bedrijfsprocessen kan. In de praktijk blijkt het vaak best mee te vallen. Een BIA begint met classificatie van bedrijfsprocessen. Welke zijn onmisbaar en welke zijn minder kritiek? Dit alles natuurlijk wel goed onderbouwd.
Een BIA maakt gebruik van diverse methodieken waarbij onder meer wordt gekeken naar:

- Financiële impact;
- imago impact;
- juridische impact;
- organisatorische en overige impact.

Bovenstaande aspecten zijn per soort nog verder onder te verdelen. Denk bij een financiële impact aan kosten (direct/indirect), cashflow, gederfde inkomsten.

Maar denk ook aan mogelijke claims: hoeveel klanten van leverancier zullen wisselen, tijdskritische periodes door het jaar of productieverlies door bederf. Financiële impact springt er vaak uit: deze is namelijk het meest concreet te benoemen. De overige impacts zijn wel degelijk van groot belang en niet te onderschatten - uiteraard mits goed onderbouw.

Slechts een deel van deze aspecten laat zich in een (schade-)bedrag vertalen. Daarom wordt bijna altijd kwalitatief beoordeeld aan de hand van een tevoren overeengekomen classificatieschaal. Bijvoorbeeld:

- Geen impact
- Geringe impact
- Aanzienlijke impact
- Grote impact
- Desastreuze impact.

Hiermee wordt het belang van het proces verbonden met het resultaat van de hele organisatie.

De BIA geeft aan welke diensten na een calamiteit met welke data binnen welke tijd beschikbaar moeten zijn. Hierop worden de eisen die de business aan IT stelt met betrekking tot dataherstel en tijdigheid bepaald.
Dit is vervolgens de onderbouwing voor het management om juiste (investerings-) keuzes te maken. Of juist om risico's inzichtelijk te maken en te accepteren. Hiermee geef je dus impliciet de touwtjes in handen aan de business om mee te beslissen over het budget voor IT. In de meeste gevallen werkt dat verhelderend, wordt IT gedwongen om inzicht te geven in kostenstructuren en begrijpt de business beter waarom sommige services niet of minder goed zijn ingericht.

Businessunits en IT-afdelingen vinden het moeilijk om dergelijke afspraken te maken.
Niet alleen IT maar ook de business zelf stelt niet altijd de juiste eisen. Daarom is het van essentieel belang dat de onderbouwing van deze eisen een van de pijlers is waarop het resultaat van de BIA stoelt. Uiteindelijk vertaalt elke eis zich in kosten. Te hoge eisen leveren te hoge investeringen die niet in businessresultaat wordt vertaald.

De waarde van data
De vraag hoeveel dataverlies je je kunt permitteren moet worden genuanceerd. Is alle data even waardevol? Of is er een classificatie aan te geven? Anders gesteld: hoe erg is het als bepaalde data op een gegeven moment niet meer beschikbaar zijn? Een van de resultaten van elke goede BIA is het bepalen van welke data vitaal is voor welk proces. En ook: binnen welke periode zijn deze data?

Het resultaat van een BIA
Zonder nog maar over een (technische) oplossing te praten geeft de BIA inzicht in de vitale bedrijfsprocessen van een organisatie. Processen die prioriteit vragen, na bijvoorbeeld een calamiteit of een storing van dat proces. Van belang is dat deze prioriteit is onderbouwd. Daarmee is het een uitstekende legitimatie voor verdere investeringen. Bovendien is een BIA het begin van een match tussen wat eigenlijk nog ingeregeld moet worden en wat al prima in orde is.

'. . . maar ook de business zelf stelt niet altijd de juiste eisen'

Het is dus een uitstekend middel om als discussiestuk te dienen voor toekomstige investeringen in IT; hiermee komt de discussie tussen Business & IT op gang. Dit lezen we als: hoe erg is het in bijvoorbeeld financieel opzicht als proces X uit de lucht is? Hierbij geldt 1 = geen impact, tot 5 = desastreuze impact.

Het houdt in dat het wegvallen van het proces na ongeveer vijf dagen op meerdere gebieden echt hinderlijk voor de organisatie wordt. Qua imago is dat stadium overigens al eerder bereikt: na drie dagen.

- Een BIA stelt voortdurend de vragen: "Waar verdienen we als bedrijf nou eigenlijk ons geld mee?" en "Wat is ons businessmodel?"
- In de praktijk wordt een BIA vaak uitgevoerd bij:
- hele grote organisaties;
- politieke organisaties (zowel overheid, semi overheid en bureaucratische ondernemingen);
- bedrijven waar business slecht communiceert met IT (zie bovenstaand betoog).

Voor deze organisaties is een BIA het meest zinvol: de business gaat eisen stellen en komt in dialoog met IT. Hoe goed dient IT het in te regelen? Met dit resultaat kan uiteindelijk ook een zinnige kosten-batenanalyse worden uitgevoerd en investeringen worden onderbouwd.

Beheer van de BIA is noodzaak
De resultaten van een eerste BIA zijn een snapshot van de bestaande situatie. De resultaten dienen te worden onderhouden: het kan goed zijn dat de impact van een calamiteit op een bedrijfsproces in de tijd wijzigt. Doordat bijvoorbeeld het belang van het bedrijfsproces door marktomstandigheden verandert. Of dat een organisatie gewoon groeit of krimpt. Ook kunnen alternatieve werkwijzen hun bruikbaarheid verliezen door toename van volumes of wijzigingen in technologie.

Onderwerp	<= ½ dag	<= 1 dag	<= 2dagen	<= 3 dagen	<= 5 dagen	<= 14 dagen	<= 31 dagen
Financieel	1	1	2	2	3	4	5
Organisatorisch	1	1	1	2	3	5	5
Juridisch	1	1	1	1	1	1	2
Imago	1	1	2	4	5	5	5
Overig	1	1	1	1	2	4	5
Conclusie	**1**	**1**	**2**	**2**	**3**	**4**	**5**

Voorbeeld: Overzicht BIA-resultaat van proces X

Als voorbeeld kan de handmatige registratie van gesprekken in een call center dienen. Het zal duidelijk zijn dat hier grenzen aan bruikbaarheid zijn.

Voorbeeld 1:
Op een researchsite wenst IT een dubbel uitgevoerd, volledig gespiegeld datacenter te bouwen. Als beursgenoteerde organisatie 'kun je daar absoluut niet omheen'. De researchafdelingen stellen door middel van een BIA vast dat ze ongeveer vier weken zonder IT kunnen. De gevolgen daarvan zijn weliswaar kostbaar, maar goed overkomelijk. Dataverlies is echter onacceptabel: het is ongelofelijk kostbaar om research die is gedaan, opnieuw uit te voeren.
De conclusie was eenvoudig: het dubbele datacenter bleek niet nodig. "*We hebben veel meer aan een goede oplossing voor onze back-up.*" Hiermee werd een discussie aangeslingerd voor het goed organiseren van de back-up. Met diverse mogelijkheden om kosten te verlagen, het risico van traditionele back-up en het vervoeren van tapes. Een voorbeeld hiervan is bijvoorbeeld *Electronic Vaulting Services* (online back-up).

'Waar verdienen we als bedrijf nou eigenlijk ons geld mee?'

Voorbeeld 2:
De IT-organisatie van een bedrijf in goederendistributie heeft zijn zaken goed voor elkaar. Een uitwijkmogelijkheid naar een tweede datacenter en de meest kritische applicaties zijn binnen 24 uur weer volledig operationeel. Elk jaar wordt getest en het Disaster Recovery Plan wordt goed onderhouden. Men vroeg zich echter af of de business zich wel bewust was van de genomen maatregelen, wat deze betekenen en of de maatregelen wel pasten bij de (wijzigende) bedrijfsdoelstellingen. Een BIA bood uitkomst. Door op efficiente wijze de business te betrekken bij de impact op een calamiteit, kon duidelijk worden gemaakt welke maatregelen waren getroffen, waar eigenlijk aanvullende maatregelen noodzakelijk waren, maar waar nu bewust een risico werd genomen.
Door de business nu te betrekken is awareness gecreëerd, begrijpt men IT beter en is het budget afgestemd op het risico. Tevens werd erkend dat er naast IT-maatregelen ook andere maatregelen noodzakelijk waren.

Voorbeeld 3:
Een IT-organisatie van een overslagbedrijf werkt met zeer gedegen professionals. Het verloop is laag; de expertise hoog. De infrastructuur heeft een upgrade ondergaan, softwareontwikkeling wordt in huis uitgevoerd. Men verwacht echter dat 70% van de IT-medewerkers binnen vier jaar met pensioen gaat. Om de kennis van de medewerkers te borgen wordt begonnen met een Business Continuiteitsplan. Al snel bleek dat de uitgangspunten voor het BCP onduidelijk waren. Voor elk plan is het van belang dat deze uitgangspunten op een duidelijke wijze worden vastgelegd. Een BIA-workshop bood uitkomst; hiermee werd ook direct inzichtelijk wat de business nu eigenlijk verwachtte. De IT-strategie was echter duidelijk en concreet: men kon voldoen aan de gestelde eisen. Vervolgens kon men het BCP gaan opstellen om zo de kennis direct te borgen.

'Dataverlies is echter onacceptabel...'

Samenvatting
Business dient eisen aan IT te stellen. Stelt de business de juiste eisen aan IT en hoe komen we daarachter?
Wat is de waarde van data?
Business Continuity Management gebruikt Business Impact Analyse (BIA) als methode om Business eisen aan IT inzichtelijk te maken.
BIA is legitimatie voor investeringen in continuïteit en levert input voor technische oplossingen.

QIY DRAAIT DE DIGITALE WERELD OM

EN STELT DAARBIJ DE BEHOEFTE VAN DE KLANT ÉCHT CENTRAAL

Marcel van Galen is oprichter Qiy Foundation. Hij is bereikbaar via info@qiy.nl.

In de wereld van vandaag wordt alles en iedereen gedigitaliseerd. Iedere Nederlander komt inmiddels voor in gemiddeld 1500 verschillende databestanden. Sociale netwerken, e-mailadressen, foto's, online bankgegevens, medische gegevens. Van iedereen is op het internet wel iets terug te vinden. Maar die informatie is alleen toegankelijk via allerlei websites en portals, die gegevens aanbieden in de vorm en structuur zoals de eigenaren van die websites en portals dat hebben bedacht. Wie herkent zich niet in de dagelijkse problematiek van meer en meer gebruikersnamen en wachtwoorden...?

Veel mensen willen informatie die achter hun gebruikersnamen en wachtwoorden leeft op allerlei portals liever zelf beheren. Ze willen weten wat er met die informatie wordt gedaan, wie die gegevens gebruikt en waarvoor. Ze willen toegang tot hun persoonlijke data om daar allerlei dingen mee te doen, zoals het combineren van die gegevens. Ze willen zelf aan het stuur zitten.
De Qiy Foundation heeft al vijf jaar geleden een visie ontwikkeld op een wereld waarin het individu écht centraal staat. En daarmee weer de regie kan nemen over zijn of haar informatie en daar bovendien slimme en handige combinaties mee kan maken. Niet een zoveelste portal, maar de wereld van morgen waarin Qiy de 'Pull' faciliteert door middel van een onafhankelijk 'independent framework' voor gewaarborgde digitale identiteiten. Dit vanuit het principe het individu te faciliteren met een gewaarborgde digitale identiteit in combinatie met een eigen omgeving.

Je digitale ik

Wat zou er gebeuren wanneer jij zelf de beschikking zou hebben over al je persoonlijke gegevens? Als jouw informatie digitaal naar je toe komt, in plaats van dat jij je gegevens overal zelf moet ophalen? En wat gebeurt er als die gegevens slim met elkaar gecombineerd kunnen worden?
Qiy is een digitale omgeving voor iedereen. Jouw onafhankelijke, veilige en intelligente digitale domein, waar je zolang als je wilt controle hebt over je eigen gegevens.
Je kunt in je Qiy zowel je eigen persoonlijke gegevens opslaan als over data beschikken van bedrijven en organisaties die voor jou relevant zijn. Afhankelijk van de mogelijkheden van de dataleverende partij krijg je toegang tot je data die bij de aanbieder bewaard blijft. Of krijg je een kopie van je data. Binnen je persoonlijke Qiy domein krijg je vervolgens inzicht in je persoonlijke situatie. Dit komt doordat bedrijven en organisaties hun kennis via applicaties aan jou aanbieden. Die applicaties kunnen je helpen inzicht te krijgen in je persoonlijke situatie doordat ze je helpen jouw rijke dataset - for your eyes only - te interpreteren.
Kennis aanbieden via applicaties is een nieuwe manier hoe bedrijven en organisaties om kunnen gaan met jouw persoonlijke data, zodat ze op een andere manier online aanwezig kunnen zijn. Ze kunnen weer écht relevant worden voor jou. Dit lost meteen een aantal problemen op: voor bedrijven vermindert hierdoor namelijk de noodzaak om meer en meer data van jou te verzamelen met alle nadelen van dien. Denk hierbij aan de bescherming van die data en de verantwoordelijkheid rondom privacy. Maar ook het feit dat die data statisch is en dus snel veroudert. Daardoor vraagt het veel kostbare uren om data ook actueel en up to date te houden. Voor bedrijven verdwijnt op termijn hiermee ook de noodzaak allerlei ongewenste boodschappen te versturen je via een steeds maar toenemend aantal kanalen. Middels Qiy ontstaat een zeer relevante vorm van 'permission based marketing'.
Qiy is een tegenbeweging op de wildgroei aan digitale gegevens en voorkomt dat privacygevoelige gegevens

> Iedere Nederlander komt inmiddels voor in gemiddeld 1500 verschillende databestanden

van mensen gaan zwerven op internet. Qiy is een ideaal vertaald naar een onafhankelijk initiatief voor iedereen.

Hoogste veiligheidscertificatie

Mickey Mouse kan geen Qiy krijgen. Als Qiy je digitale ik is, dan is het vreemd als jij twee Qiy's zou kunnen hebben of dat een stripfiguur een persoonlijk digitaal domein heeft. Qiy is de gewaarborgde digitale identiteit van het individu. Om een Qiy te krijgen dien je jezelf te identificeren op een voldoende hoog niveau. Qiy werkt met de Europese Stork-levels. Daarin worden vier niveaus benoemd, van een eenvoudige gebruikersnaam/wachtwoord aanmelding zonder controle tot een vier sterren identiteit, die bestaat uit de bevestiging van een derde partij, die jouw fysieke verschijning heeft gekoppeld aan je officiële identiteitsbewijs en aan je Qiy. Qiy accepteert een identiteitsvaststelling vanaf Level 2: een erkende derde partij bevestigt dat jij bent die je zegt dat je bent.

De Qiy infrastructuur is geen centrale component, maar als een framework opgezet voor een netwerk van los van elkaar functionerende nodes. Ontworpen op het kunnen omgaan met falende componenten: geen single points of failure en overzichtelijke deelsystemen. Het Qiy framework vormt de basis voor de maatregelen ten behoeve van de beveiliging en de privacy-bescherming. Ook hier geldt een multidimensionale strategie; niet alleen ten aanzien van toegang en rechten, maar juist 'behavior driven'; ongebruikelijk gedrag kunnen detecteren en daar op kunnen ingrijpen. De beveiliging aan de voorkant werkt met twee-factor authenticatie bij inloggen, aangevuld met adaptieve authenticatie. Twee-factor authenticatie betekent dat er iets is wat je wéét en iets wat je hébt. Adaptieve authenticatie houdt in dat het systeem steeds de vinger aan de pols houdt ten aanzien van 'verwacht gebruik' gedurende het gebruik van het persoonlijk digitaal domein. Is de PC bekend waar vandaan ingelogd wordt? Is het IP-adres te verwachten? Is het ritme van de toetsaanslag bekend? Vele kenmerken kunnen hier onderdeel van worden gemaakt. Daarnaast werkt Qiy met encryptie strategieën, dynamische autorisatie en gedistribueerde gegevensopslag.

> Met Qiy verandert Customer Relationship Management daadwerkelijk in Customer Managed Relations

Privacy by design

Een andere belangrijke kernwaarde van Qiy is dat de infrastructuur en zelfs de hele organisatie is ingericht op basis van 'privacy by design' principes. Concreet betekent dat bijvoorbeeld dat identificerende data losgekoppeld wordt van algemene data die van het individu is. Feitelijk: salarisdata kan worden afgeleverd in het persoonlijke domein van het individu zonder dat daar een naam of een adres bij staat. Dat heeft tot gevolg dat zelfs áls een server wordt gehackt, er slechts een berg versleutelde data zonder identificerende gegevens te vinden is. Bovendien is het straks mogelijk je eigen beheer over je gegevens te organiseren. Voor welk onderdeel wil je dat welke authenticatievraag wordt geactiveerd? Je kunt er bijvoorbeeld voor kiezen zelf een extra pincode toe te voegen aan een financiële applicatie. Ondanks alle veiligheidsmaatregelen weten we allemaal dat de gebruiker de potentiële zwakste schakel blijft in de beveiliging van het persoonlijke

domein. Compromittering zal in het geval van Qiy beperkt blijven tot het betreffende domein. Dit heeft geen invloed op het functioneren van het gehele systeem.
In mei 2011 werd het concept bekroond met de European Identity Award in de categorie privacy. Qiy is privacy gecertificeerd op het hoogste niveau op het gebied van security en privacy met het keurmerk Privacy-Audit-Proof van Nivra/Norea.

Wat betekent Qiy voor bedrijven?
Qiy biedt nieuwe mogelijkheden voor bedrijven die zich aansluiten, waaronder: de gewaarborgde digitale identiteit van het individu, actuele gegevens, kennis in contact brengen met een rijke dataset van de gebruiker en daarmee relevantie aantonen, aandacht voor duurzaamheid door vermindering van het gebruik van papier en misschien wel het belangrijkste: een heel nieuwe betekenis van permission marketing.
Met Qiy zit de consument aan het stuur. Qiy verandert daarmee het begrip Customer Relationship Management daadwerkelijk in Customer Managed Relations.
Op deze manier biedt Qiy bedrijven:

- de mogelijkheid data beschikbaar te stellen aan de klant;
- de kans gericht, integer, relevant en op consumenten te kunnen benaderen op uitnodiging;
- de mogelijkheid om op een intelligente manier een hoogwaardige digitale relatie aan te gaan met consumenten;
- de gelegenheid additionele waarde te genereren vanuit het specifieke kennisgebied van het bedrijf;
- verlaging van marketing- en distributiekosten;
- vergaande databeveiliging die individuele bedrijven zich veel moeilijker kunnen permitteren;
- de mogelijkheid maatschappelijk betrokken te zijn;
- een rol in het dagelijkse digitale leven van de gebruiker.

Qiy en overheden
De overheid kan de burger helpen door hem zijn gegevens middels Qiy als Trust Framework toe te vertrouwen, met een waarmerk dat die gegevens echt afkomstig zijn van de overheid. De overheid kan de burger applicaties bieden waarmee hij kan acteren op basis van zijn eigen gegevens. Zodanig dat de burger weet dat de bescherming van zijn persoonsgegevens is gewaarborgd. De burger kan om te beginnen laten weten of zijn gegevens correct zijn. Hierdoor neemt het foutpercentage in deze gegevens bij de overheidsinstantie af. Daarnaast kan de overheidsinstantie de benodigde informatie rechtstreeks aan de burger zelf vragen zonder achter zijn rug deze informatie te hoeven toetsen bij de GBA of een van de andere databases van de overheid.

Jouw Qiy, dat ben jij online!

Een goede en verantwoorde omgang met persoonsgegevens is een essentieel element van de vertrouwensrelatie tussen de burger en de overheid.
Op deze manier biedt Qiy overheden:

- de mogelijkheid data beschikbaar te stellen aan de burger;
- de kans een maatschappelijke beweging, die het gebruik van internet veiliger maakt voor haar burgers, te ondersteunen;
- de mogelijkheid tot betere dienstverlening;
- overzicht en inzicht in publieke en private data met positieve effecten op de noodzakelijke zelfredzaamheid van de burger.
- verbetering van de kwaliteit van lokaal bestuur door toegankelijker, gebruiksvriendelijker, transparanter, eenduidiger en begrijpelijker overheidsinformatie;
- verlaging van de IT-kosten van de overheid;
- de mogelijkheid te voldoen aan de privacy wetgeving;
- aandacht voor duurzaamheid door vermindering van het gebruik van papier;
- de kans om kennisintensieve innovatie voor burgers en de BV Nederland mogelijk te maken met een uitstraling en een eventuele uitbreiding in Europa en de rest van de wereld.

Eind 2011 ontving Qiy de Accenture Innovation Award Public Services.
Een onafhankelijke vakjury, die uit zeer gerespecteerde namen uit de overheid bestaat, sprak zich uit over de innovatie, het potentieel en het toekomstige succes van Qiy.

"Qiy laat met dit innovatieve internetconcept zien dat het een sterke visie heeft op informatiemanagement en -beveiliging. Bovendien speelt het hiermee ook in op de ontwikkeling dat steeds meer informatie wordt bewaard in de cloud. Controle en beveiliging zijn hierbij essentieel. EMC is sinds de oprichting van Qiy als partner bij het bedrijf betrokken. Bovendien deelt zij het uitgangspunt dat de gebruiker als eigenaar centraal zou moeten staan in het beheer van zijn informatie. Op deze manier kunnen zowel bedrijven als consumenten zorgen dat er verantwoordelijk wordt omgegaan met alle informatie die wordt gecreëerd, gebruikt, verspreid en beheerd."
Frans Rahms, VP Noord Europa EMC

"Voor Qiy is een 'thought leadership' positie weggelegd die een wereldwijde impact zal hebben op de wijze waarop individuen, bedrijven, organisaties en maatschappijen in de toekomst met elkaar communiceren. De maatschappelijk relevante innovatie van Qiy voorziet in de behoeften van individuen om digitale informatiestromen te kunnen beheersen."

Andrea Vogel, Partner bij Ernst & Young Accountants

Auteur: Robert L. Garskamp is founder of IDentity.Next en ook werkzaam als projectmanager bij Everett, hij is per e-mail bereikbaar via robert@garskamp.com

IDENTITY NEXT

Voor het 2e jaar in successie, vond IDentity.Next'11 op 9 November 2011 plaats in het 7AM conferentie centrum in Den Haag, de stad van recht en veiligheid. Net als vorige keer kwamen er meer dan 100 deelnemers bijeen om zich te laten inspireren, om te netwerken en ontwikkeling met elkaar te kunnen uitwisselen rondom het onderwerp 'de digitale identiteit'. Het PvIB was een sponsor van dit evenement, waardoor er ook PvIB-leden aanwezig waren. Het event hanteerde ook dit jaar weer de succesvolle un-conference formule. Het was duidelijk dat de meeste deelnemers zich deze keer hadden voorbereid. Ze kwamen gewapend met onderwerpen naar het event. Het un-conference format zorgt ervoor dat er ruimte is voor ontmoetingen met kennisexperts, samenwerking, interactie, discussie en creativiteit. Natuurlijk hangt het voor een groot deel van jezelf af wat je als deelnemer hieruit haalt. Tijdens IDentity.Next is er mogelijkheid om te luisteren en ook spreken met deskundigen en professionals en ook (heel belangrijk) zelf deel te nemen aan debatten en discussies. Met het un-conference format, wordt de agenda - in relatie tot de thema's – op de dag zelf vastgesteld.

De belangrijkste missie van IDentity.Next is een open en onafhankelijk platform te kunnen bieden dat staat voor ondersteuning en faciliteren van innovatieve benaderingen in de wereld van de digitale identiteit. Met als voornaamste doel het dissimineren van kennis, expertise en ervaring door het organiseren van evenementen en workshops. Gebaseerd op een verscheidenheid aan thema's, gemaakt voor en door experts binnen de wereld van IT, Business en Marketing.

Na de opening door Robert Garskamp – founder van IDentity.Next – werd de keynote presentatie gegeven door Jan Willem van Dongen. Hij is de bestuursadviseur van Gerdine Keijzer-Baldé, directeur van het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR), die helaas zelf niet aanwezig kon zijn wegens een reis naar Curaçao. Het agentschap maakt onderdeel uit van het Ministerie van BZK. Tijdens zijn keynote-presentatie gaf Jan Willem de aanwezigen een kijkje in de keuken van BPR. Zo wist hij te vertellen dat de diensten van BPR uit een betrouwbare registratie en het leveren van persoonsgegevens en reisdocumenten bestaan. Deze diensten worden aan 418 gemeentes, 800 overheidsinstellingen en Caribisch gebied aangeboden. Om dit te kunnen leveren onderhoudt BPR hiervoor dan ook diverse systemen, zoals: Gemeentelijke Basis Administratie (GBA), Persoonsinformatie voorziening Nederlandse Antillen en Aruba (PIVA), burger service nummer (BSN) en het systeem dat de reisdocumenten produceert en oplevert. Jan Willem had interessante cijfers te melden: in 2011 zijn er 1,8 miljoen paspoorten en 1,5 miljoen identiteitskaarten uitgegeven, waarbij het feit dat de identiteitskaart een tijdje gratis was een gekleurd beeld geeft. Ook blijkt dat het GBR nog veel uitdagingen voor zich heeft vanwege constante

Robert geeft het woord aan Jan Willem van Dongen (BPR)

politieke druk. Voorbeelden hiervan zijn het kunnen blijven bieden van een hoge kwalitatieve en actuele gegevensadministratie, het verplicht afnemen van BAG (Basis registratie Adressen en Gebouwen) door het GBA (Gemeentelijke Basisadministratie persoonsgegevens), consolidatie en continue verbetering van de infrastructuur. Jan Willem beëindigde zijn verhaal met de stelling dat de uitvoering en verbeteringen binnen GBR stap voor stap op een gedegen wijze moeten worden uitgevoerd. Het is ook een kwestie van doen, concludeert hij. Overigens leidde de presentatie van Jan Willem tot pittige discussies met de aanwezigen. Onder andere vanwege zijn stelling dat het GBA voor 98% administratief betrouwbaar is. Hoe het in het echt is, is niet bekend... Ook de opmerking dat het BSN niet de burger van dienst is, leverde de nodige blikken van herkenning op. Het was al duidelijk dat men niet voornemens was om achterover te leunen en alleen maar te luisteren. IDentity.Next was echt van start gegaan…

Net als bij elk ander event is netwerken een belangrijk onderdeel om kennis en ervaring te delen. Tijdens de breaks werd hier veelvuldig gebruik van gemaakt. Visitekaartjes werden te pas en onpas uitgewisseld (waarom is hier trouwens nog geen goed alternatief voor?) In de ochtend waren verschillende breakout sessies gepland. Deze sessies behelsten verschillende thema's die nauwe affiniteit hebben met de wereld van de digitale identiteit. De thema's waren:

'**ecitizen':** waarin de vraag centraal staat of een single identity voor burgers en werknemers de beste weg is om van de volgende generatie eOverheidsdiensten gebruik te maken. De initiatieven op dit vlak zijn vaak even veelbelovend als controversieel,

'**mobileme':** dit thema brengt mobiliteit en identiteit samen. Als we onderweg zijn bellen we, sturen we e-mails en sms-jes en geven we betaalopdrachten. Het digitale identiteitsvraagstuk wordt in deze context steeds complexer. Wie heeft de controle over informatie en in hoeverre is dat noodzakelijk? En is mijn mobieltje misschien wel het ideale middel om mijn digitale identiteit te beheren?)

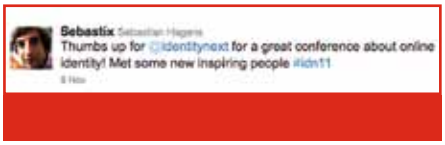
'**Social consumer':** de laatste ontwikkelingen op het gebied van social commerce (ecommerce met gebruikmaking van sociale media) gecombineerd met user-centric identity

'**private eye':** over het privacy aspect. Ervaren we het wel als een probleem? En zo ja, wie moet daar dan iets aan doen? Internetproviders, sociale netwerken en overheidsdiensten maken dagelijks gebruik van informatie. Maar waar ligt de regie als het om privacy gaat?

Netwerken bij Identity.Next 2011

Ook deze keer was de programmacommissie (met o.a. Eva Kassenaar en Maarten Wegdam) erin geslaagd een internationaal gezelschap van professionals en experts hun visie en mening te laten geven en delen over de wereld van de digitale identiteit.

Marnix Dekker praat over mobile security



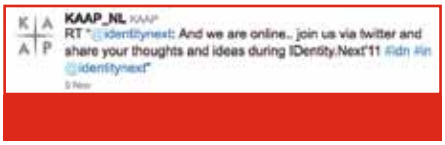
UN-conference

Na de biologische lunch nam Kaliya Hamlin (ook bekend als Identitywoman) het heft ook deze keer weer in handen voor het faciliteren van het un-conference deel tijdens IDentity.Next'11. Kaliya heeft jarenlange ervaring met het modereren van un-conference events. Bij de un-conference wordt de 'Open Space' gebruikt. Open Space vertaalt zich naar open ruimte en werkt geheel zonder agenda. Het is een raamwerk dat de juiste condities schept voor een dynamisch en creatief proces van discussie en samenwerking. Het concept zorgt ervoor dat iedereen aan het eind gezegd heeft wat hij/zij wilde zeggen, met een uitgebreid verslag van de discussies, veel netwerken onderling en het uitwisselen van ideeën en het ontwikkelen van visies tussen de aanwezigen. De un-conference start altijd met een introductie en uitleg van de methode, het vaststellen van de onderwerpen en dan het opstellen van de agenda. Na wat aarzelingen kwamen

de aanwezigen op stoom en was binnen een half uur de agenda vastgesteld. Hierna ging men uiteen en sloot men aan bij de eerste sessies. Een greep uit de agenda van de un-conference:

- Everyone has a right to privacy, but not everyone has a right to anonymity
- mobile devices as a identity manager
- How to deal with multiple levels of assurance - at the same time.
- mobile wallets online, nfc, tsm etc…
- do you really get an identity by using a social network?
- Risk based authentication (pros and cons)
- What incentives are there/should there for commercial organisations to support privacy for individuals
- Your identity does not die with you.

Tijdens deze dag werd er weer goed getwitterd (met de hashtag #idn11). Dit leidde zelfs tot discussies met anderen die helaas niet aanwezig konden zijn bij deze editie, maar wel via sociale media de discussie konden volgen en voeren. Wederom werd de kracht van social media hierin aangetoond.



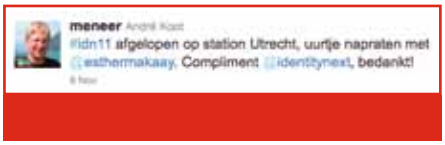
Novay Digital Identity Award

Tussen de un-conference sessies door vond ook de uitreiking van de Novay Identity Award plaats. Een award voor het beste nieuwe concept of product op het gebied van digitale identiteit. Opnieuw was er een jury samengesteld onder leiding van Hermen van der Lugt (directeur Novay). De overige juryleden waren: Gerrit Jan Bloem (Ziggur), Jaap Kuipers (PIMN) en Dennis van Ham (KPMG).
Uit inzendingen vanuit vijf landen waren vier genomineerden geselecteerd: het Australische edentiti, het Deense WAYF en de Nederlandse Qiy en tiQR.

Edentiti (http://www.edentiti.com) heeft een systeem voor het verifiëren van identiteiten aan de hand van diverse betrouwbare online databronnen. De gebruiker bepaalt zelf welke. Qiy (http://www.qiy.com) is een Nederlands initiatief dat de gebruiker een veilige omgeving biedt voor het opslaan van persoonlijke data. De gebruiker bepaalt ook welke bedrijven toegang hebben tot die data. WAYF (http://www.wayf.dk) ofwel 'Where Are You From?' is een identiteitsfederatie die meer dan 90 serviceproviders verbindt met 130 identity providers in het Deense onderwijs. WAYF is een pionier met onder meer een 'user consent module' en real-time berekening van de economische voordelen die het gebruik van de federatie oplevert. De organisatie draagt bij aan open source. tiQR (http://tiqr.org) is een open-source, op standaarden gebaseerde authenticatie-oplossing van SURFnet. Het mobieltje wordt hierbij gebruikt om een QR-code op een webpagina te scannen, waardoor een gebruikersvriendelijke two-factor authenticatie in gang wordt gezet.

De genomineerden mochten hun innovatieve oplossing in een korte pitch presenteren. Daarna was het aan Hermen de beurt om de winnaar van de Novay Digital Identity Award 2011 bekend te maken. Het was een moeilijke keuze maar uiteindelijk werd Edentiti uit Australie als winnaar door de jury geselecteerd. Kevin Cox (oprichter van eDentiti) nam deze zeer mooie award (wederom een mooi beeld ontwerpen door Alexandra Veneman) op een virtuele manier in ontvangst. Kevin kon helaas niet fysiek bij de uitreiking in Den Haag aanwezig zijn en de award zal op een later tijdstip alsnog door hem in ontvangst worden genomen. Kevin heeft beloofd dat hij op de volgende editie van IDentity. Next aanwezig zal zijn.

Na de roundup van de unconference door Kaliya in de plenaire zaal en formele afsluiting door Robert Garskamp werd deze dag afgesloten met een netwerkborrel die ondanks de lange dag nog erg goed werd bezocht. Hiermee kwam een inspirerende dag ten einde. Naar verluidt gingen de inhoudelijke discussies hierna zelfs nog lang door (zelfs op het station).



Meer informatie over IDentity.Next: http://www.identitynext.nl

Herman overhandigt de award aan de virtueel aanwezige winnaar

ACHTER HET NIEUWS - MOBIELE MALWARE

In deze rubriek geven enkele van de IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems inzake informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en geeft niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Vragen en opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

In het nieuws was volop aandacht voor berichten over mobiele malware. Twee berichten sprongen eruit: Juniper publiceerde een rapport over toename in malware op het Android platform[1]. Elders in dit blad een uitgebreider artikel hierover. Het tweede is van onderzoeker Trevor Eckhart die een analyse deed over extra activiteit op zijn Android toestel[2]. Carrier IQ reageerde vrij zwaar met een rechtzaak tegen Trevor, maar trok zich iets terug[3]. Deze keer reageert naast de redactie ook Mark van Cuijck, winnaar van de Joop Bautz Security Award.

Mark van Cuijck

Er zijn veel overeenkomsten tussen software- en malware-industrie. In beide industrieën worden salesprocessen geoptimaliseerd, vinden zowel grootschalige als gerichte marketingcampagnes en R&D-activiteiten plaats. Het belangrijkste verschil is het product: bedrijven in de software-industrie voegen waarde toe voor de klant. Bedrijven in de malware-industrie proberen geld te verdienen ten koste van derden.

Beide industrieën zijn actief in de mobiele wereld. Hoewel een mobiel toestel veel weg heeft van een PC - Android draait bijvoorbeeld bovenop een Linux-kernel - moeten veel bedrijven ontdekken hoe dit nieuwe platform in te zetten om geld te verdienen. Een aantal bedrijven is hier al succesvol in.

De R&D-molen van de malware-industrie proberen bestaande en nieuwe concepten uit. Enerzijds wordt gewerkt aan distributiemodellen: malware verspreiden via de Android Market of via kwetsbaarheden in de browser. Anderzijds zijn er experimenten hoe toegang tot deze apparaten kan worden omgezet in winst.

De toekomst wijst uit of de malwaredreiging geen hype of stemmingmakerij is. Het kan even duren, maar bedreigingen komen pas wanneer ontwikkelaars ontdekken hoe ze effectief kunnen werken. De malware-industrie heeft een achterstand, die zonder onze actie wordt ingehaald.

André Koot

Mijn eerste computer kocht ik in 1982. Na het spelen van de eerste spelletjes dook ik al snel in Basic (10 PRINT 'Hello World'; 20 GOTO 10). Meteen daarna ging ik het romgeheugen in om allerlei trucs uit te halen zoals Sinclair ze niet had bedoeld. Sindsdien ben ik altijd baas geweest over mijn eigen computers, administrator, root. Prettig idee.

Met die mogelijkheid ontstaan ook risico's, die leiden tot overlast voor derden. Virusinfecties, spambots; je hebt er zelf weinig last van. Maar met die smartphones is iets anders aan de hand. Die gebruiken schaarse en (voor ons) dure netwerken. En gaat er dan iets fout, heb je er zelf wél last van. Baas worden over je eigen smartphone is dan ook niet altijd verstandig.

En toen verscheen Carrier IQ. Stuurt gegevens naar je provider om techniek te monitoren. Als je daar vanaf wilt, moet je wel weer de baas over je computer worden. Beter niet doen dus, dat 'rooten' of 'jailbreaken'? En er op vertrouwen dat je provider ook met jou het beste voor heeft...

Lex Borger

Te beginnen met Carrier IQ: vreemd aan dit verhaal is, dat je gewoon niet weet wie je moet geloven. Trevor laat duidelijk zien wat er op zijn toestel kan, Carrier IQ maakt duidelijk dat dit niet de bedoeling is. Telecomproviders staan hier tussenin. Gelukkig geen Nederlandse providers. Ze wisten gewoon niet hoe snel ze dit formeel moesten verklaren. Kennelijk zijn er elders wel degelijk providers die toestellen leveren met goedkope, knullige implementaties van software Carrier IQ. Ik geloof dat een provider veel heeft aan het monitoren van telefoonontvangst. Maar laat dit dan 'opt-in' zijn, of minstens 'opt-out'. Er zijn genoeg softwareproducten die dit beleefd vragen.

Wat malware op Android betreft: het lijkt er voorlopig op dat Apple en Blackberry met hun gesloten model malware beter kunnen mijden. Maar de race is nog lang niet gelopen. Blijven Apple en Blackberry in staat op eigen kracht hun OS-en veilig te houden bij doorontwikkeling? Is Google in staat alle partijen in het Androidkamp te verenigen tegen malware? Wordt vervolgd.

Referenties

[1] *Juniper Global Threat Center,* **Mobile Malware Development Continues To Rise, Android Leads The Way**, *http://globalthreatcenter.com/?p=2492*

[2] *Trevor Eckhart on YouTube,* **Carrier IQ Part #2**, *http://www.youtube.com/watch?v=T17XQI_AYNo*

[3] *Carrier IQ,* **Press Releases and Trade News**, *http://www.carrieriq.com/company/news.htm*

REGISTER INFORMATIEBEVEILIGING 2011

● Artikel ▼ Verslag ■ Interview

Artikelen

COLOFON

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
Lex Borger (hoofdredacteur, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.nl

Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

Abonnementen 2012
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

BEN IK NOG OP DE GOEDE WEG?

Soms ben je een beetje aan het surfen op het internet en dan wordt je blik ineens gevangen door een pakkende kop, namelijk: '8 gevraagde IT-vaardigheden'. Je begint onmiddellijk te lezen en aan het eind van het artikel kom je tot de conclusie dat er in al die jaren helemaal niets is veranderd. Niets is iets te zwaar aangezet, maar de veranderingen zijn met name te vinden in de details. Een groot aantal jaren waren deze functies er ook al, maar toen benoemden wij ze anders. Toch leuk om dit artikel, wat met input van Computerworld, Forrester en Robert Half Technology is opgesteld, eens te analyseren.
Op nummer 1 staat applicatieontwikkeling.
Niet echt een grote verrassing. We zijn immers nog steeds niet tevreden met de software die ons kant en klaar wordt geleverd. We willen er altijd wel een bultje op bouwen omdat ons bedrijf namelijk zo uniek is.
De grote stijger, de businessanalyse, staat op de tweede plaats. Niet vreemd, omdat wij IT-ers datgene bouwen waarvan we denken dat goed is voor de gebruiker. Deze businessanalisten zijn er volledig voor de gebruiker. Zowel om de wensen en eisen te inventariseren als te laten implementeren.
Helpdesk staat op de derde plaats en die zal in onze steeds complexere infrastructuren een steeds belangrijkere rol innemen. Een 'normale' gebruiker heeft toch al moeite de weg te vinden.
Op nummer vier staat Networking - en dan specifiek de virtualisatietovenaars - zullen meer en meer worden gevraagd. Een logische reactie: beheersbaarder, minder hardware, snellere vervanging van hardware mogelijk en dergelijke.
Op de vijfde plaats staat de business intelligence. Ook dit is niet zo vreemd. Beslissers willen gewoon gebruik maken van de data die in hun bedrijf is verzameld om besluit-ondersteunend te kunnen zijn.
Als zesde staat WEB 2.0, volstrekt logisch: social media, webontwikkeling en cloud-ontwikkelingen zorgen er immers voor dat bedrijven (nog) dichter en vindbaarder op internet staan.
Als zevende staat dan eindelijk ons vak Beveiliging genoemd. Gezien de afgelopen jaren geen gekke positie. We ervaren een grote mate van onveiligheid. Ik lepel de voorbeelden van gehackte bedrijven niet op. Het mag toch als bekend worden verondersteld dat er nog veel meer bedrijven lek zijn? Die hebben het geluk gehad nog niet door de buitenwereld te zijn ontdekt. Lektober (een geweldig initiatief van Webwereld) was helaas een groot succes. De heren van de website Webwereld hadden er dan ook geen enkele moeite mee er een Lekvember achteraan te doen.
Op de achtste plaats staan de specialisten van onze legacysystemen. Het ontbreken van deze specialisten is volgens mij de grootste continuïteitsdreiging. Grappig, we hebben van die oude systemen die al jarenlang draaien en die om wat voor reden dan ook niet weg of vervangen kunnen worden. Het kan ook zijn dat we geen investering wíllen doen om de oude systemen te vernieuwen. Leuk om te zien dat de babyboomgeneratie met hun Cobol- en RPG-kennis inmiddels als zeer schaars en zeer gewild worden gezien. De lange grijze baarden hebben kennis in het hoofd, wat nergens meer wordt onderwezen.

De huidige studenten komen met veel kennis van de Universiteiten en Hogescholen af, maar kunnen helaas op geen enkele manier goed programmeren. Ik weet niet tegen hoeveel schenen ik nu schop, maar dat spijt mij dan. Deze kunstenaars waren in staat om slechts in beperkte computergeheugens hun opdrachten te schrijven. Ter informatie voor degenen die nu over hun schenen wrijven: dit was vroeger een schaars goed. Deze ondergewaardeerde medewerkers hadden slechts aan een paar KB aan geheugen voldoende om de belangrijkste bedrijfsprocessen te automatiseren (dat heette toen nog geen Informatie Technology). Programmatuur was eenvoudig te testen en reageerde uiteindelijk altijd op dezelfde manier. Uiteraard was het allemaal meer basaal dan vandaag de dag. En de 'graphical user interface' was slechts een CUI (character user interface). Wil je snel data opzoeken en invoeren, dan zit een muis je vaak alleen maar in de weg. Niet iedereen zal zich de schermen met de groene letters herinneren, maar vaak waren deze systemen snel, robuust en uiterst betrouwbaar. Het lijkt erop dat de verhouding medewerkers met legacy-ervaring en security-mensen omgekeerd evenredig is: hoe minder legacy, hoe meer beveiligers.
Op zich past die conclusie ook wel in mijn beeld van de afgelopen jaren. Alle techniek moet er steeds mooier uitzien. Jammer genoeg wordt de functionaliteit wel eens uit het oog verloren. Als voorbeeld noem ik tekstverwerkers waarvan ik alleen de spellingschecker gebruik en de andere 1129 functies nog nooit heb aangeraakt.
Geef mij maar gewoon mijn CUI-tekstverwerker als WordPerfect of DisplayWrite. Maar ja, mijn grijze baard is dan ook wel heel erg lang…

Berry

BEFINE cryptshare®

BEFINE cryptshare® For Microsoft Outlook 2010

BEFINE cryptshare® For Lotus Notes

There are better ways to transfer files securely!

- Easily send large files up to 2GB
- Confirmation of file download
- E-Mail encryption
- Simple and secure file transfer

www.cryptshare.com

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Cryptshare. Neem contact op via sales@crypsys.nl of via 0183 62 44 44 voor een gratis evaluatie.

CRYPSYS data security