Het Nederlandse 'Internet of Things' volgens Censys
7 december 2017

Het Internet bestaat uit miljarden individuele netwerken die via routers met elkaar in verbinding staan. Het gaat om kleine netwerken in een gebouw maar ook om wereldwijde netwerken. Elk netwerk heeft een beheerder. Dit kan een Internet Service Provider (ISP) zijn, maar bijvoorbeeld ook een universiteit of een bedrijf. Beheerders kunnen ook meerdere netwerken beheren. Een verzameling van netwerken die onder het beheer staat van één beheerder wordt een 'Autonomous System' (AS) genoemd. Een 'Regional Internet Registry' (RIR) wijst elk AS een uniek identificerend nummer (ASN) en een landcode toe.

Medio oktober 2017 telde Nederland 764 'Autonomous Systems' die onder het beheer stonden van 712 verschillende beheerders. De meeste beheerders beheerden één AS. Vijf beheerders voerden het beheer over meer dan twee 'Autonomous Systems'.

Het aantal 'Autonomous Systems' per land wordt door de OESO gezien als een maatstaf voor de mate van marktcompetitie binnen een land. Het geeft aan in hoeverre enkele bedrijven in staat zijn om de routing van internetverkeer te controleren. In 2010 telde Nederland 2,36 AS-nummers per honderdduizend inwoners. Dat aantal steeg verder naar 3,01 in 2012 en 3,58 in 2014.[1] In oktober 2017 was dat aantal gestegen naar 4,47 AS-nummers per honderdduizend inwoners.

De vanuit Nederland beheerde netwerken telden in totaal tezamen 1.376.015 servers of apparaten die op dat moment via een IP-adres publiek toegankelijke diensten leverden op het internet. In dit artikel waarin we ingaan op een aantal eigenschappen van het Nederlandse 'Internet of Things' (IoT), op basis van een op Internet beschikbare bron, beperken we ons met het geven van informatie tot deze 'Things' die zich dus op het Internet kunnen identificeren via een uniek IP4-adres.[2]

'Internet of Things'
Over wat precies gerekend moet worden tot het IoT wordt verschillend gedacht.[3] Definities worden vaak vooral beïnvloed door de invalshoeken die door de opsteller gekozen worden en maken daarmee zo'n definitie niet waardevrij. De in dit artikel gekozen aanpak is vooral ook praktisch van aard. De analyse is namelijk gebaseerd op een bron (Censys) die op basis van IP4-metingen het IoT wereldwijd in kaart brengt. Een andere optie is er ook niet. Het is namelijk niet mogelijk om via directe metingen op het Internet te komen tot inzichten in de ruimste definitie van IoT: alle apparaten die zijn aangesloten op het Internet. De schatting daarvan lopen uiteen, maar het lijkt te gaan om miljarden en wellicht tientallen miljarden apparaten.
Een belangrijk aspect in de beschrijving van het IoT is de onafhankelijkheid van menselijk handelen. Apparaten reageren zelfstandig op prikkels (informatie) die zij via het Internet dankzij een IP-adres kunnen ontvangen, of besluiten zelfstandig prikkels af te geven aan het IP-adres van andere apparaten. Daarom worden de volgende apparaten die wel kunnen communiceren – maar alleen door menselijke tussenkomst – niet tot het IoT gerekend: desktop computers, laptops, tablets, smartphones, traditionele mobiele telefoons, televisies, DVD-/MP3-spelers en game consoles. Deze apparaten worden ook niet waargenomen in de methodiek van Censys. Maar niet vergeten moet worden dat ook apparaten die achter een eigen netwerk met Internet verbonden zijn risico's lopen. Deze risico's zijn echter niet het onderwerp van deze analyse.

Censys
Censys is een onafhankelijk organisatie en ook de naam van een website met een zoekmachine waarop informatie over 'hosts' en netwerken gegevens beschikbaar worden gesteld. Zeer frequent en vaak zelfs dagelijks maken de medewerkers van Censys - die de activiteiten ooit startten als onderzoeksproject bij de universiteit van Michigan – scans van het Internet. Met behulp van zeer snelle computers en speciaal

ontwikkelde software (ZMap en ZGrab) worden binnen een mum van tijd wereldwijd alle IP4-adressen gescand op kwetsbaarheden. De data wordt belangeloos gedeeld met de onderzoekswereld mede om te voorkomen dat te veel organisaties zelf het Internet gaan scannen en op den duur steeds meer partijen scans van hun apparaten gaan verhinderen. Behalve interactieve zoekopdrachten via de website kunnen ook zeer grote databestanden gedownload worden. Dit artikel is gebaseerd op zo'n download en bevat de data die betrekking heeft op 13 oktober 2017.[4]

AS versus locatie

De omvang van het Nederlandse 'Internet of Things' (IoT) - geredeneerd vanuit de AS-indeling - bestaat dus uit bijna 1,4 miljoen 'Things'. Het merendeel (95 procent) daarvan betreft servers waarop bijvoorbeeld ook websites gehost worden die in geval van 'shared hosting' functioneren via een gedeeld (server) IP-adres. Elke server kan op zijn beurt ook weer onderdak bieden aan vele IP-adressen. Bij een server hoeft ook niet altijd gedacht te worden aan een fysieke computer. Zware fysieke computers kunnen softwarematig opgedeeld worden in meerdere virtuele servers die dan weer bereikbaar kunnen worden gemaakt via een eigen IP-adres. Dit verklaart het verschil in aantallen IP-adressen waarover in dit artikel gerapporteerd wordt en de aantallen beschikbare IP-adressen. De IP-adressen waarover we in dit artikel rapporteren representeren 'hosts'. Hosts zijn technisch gezien de kleinste zelfstandige onderdelen van het internet die voorzien zijn van een uniek IP-adres en zelfstandig data creëren, opslaan, ontvangen of verzenden (of een combi van meerdere van deze zaken). Om die taken te kunnen verrichten beschikken 'hosts' over een softwarematige of hardware matige faciliteit om transmissies te herkennen, te verwerken of door te sturen naar andere netwerk 'hosts'. Elke 'host' beschikt over een eigen besturingssysteem dat gehackt kan worden en daarom goed beveiligd moet worden om misbruik te voorkomen. Communicatievoorzieningen zoals een wireless local area network (WLAN) access point hebben geen IP-adres en worden beschouwd als onderdeel van het fysieke netwerk waarop zij zijn aangesloten en dus niet als 'hosts'.

Tabel 1. IoT: 'Things' gelinkt met een Nederlands 'Autonomous System', oktober 2017

Locatie	abs.	%
Nederland	1 204 265	87,5
Verenigde Staten	33 170	2,4
Kroatië	19 200	1,4
Rusland	17 605	1,3
Duitsland	8 800	0,6
Verenigd Koninkrijk	7 450	0,5
Roemenië	4 350	0,3
Zuid-Afrika	4 095	0,3
Noorwegen	3 420	0,2
Zweden	3 375	0,2
België	2 530	0,2
Tsjechië	2 475	0,2
Frankrijk	2 345	0,2
Overige landen	62 935	4,6
Totaal	1 376 015	100

Bron: Censys.io, bewerking CBS

Van IP-adressen die toegerekend werden aan een vanuit Nederland beheerd AS was ook bekend waar de server of het apparaat zich daadwerkelijk fysiek bevond. 1.204.278 apparaten of servers (87,5 procent) bleken fysiek in Nederland aanwezig te zijn. Daarna kwamen als locaties naar boven: de Verenigde Staten (2,4 procent), Kroatië (1,4 procent), Rusland (1,3 procent), Duitsland (0,6 procent) en het Verenigd Koninkrijk (0,5 procent). Van 2,7 procent van de servers of apparaten was de locatie onbekend.
Het Nederlandse 'Internet of Things' kan in plaats van op basis van 'Autonomous Systems' ook bekeken worden vanuit het perspectief locatie. Onder IoT wordt dan verstaan de 'Things' die fysiek in Nederland aanwezig waren ongeacht of zij gelinkt waren aan een netwerk dat viel onder een AS dat tot het Nederlandse domein gerekend wordt. Dit perspectief levert een aanmerkelijk groter IoT op. Het aantal apparaten bedraagt niet meer circa 1,4 miljoen maar wordt dan opeens ruim 3,2 miljoen. Opvallend is dat de meeste 'Things' – bijna 63 procent – die in Nederland aanwezig zijn, gelinkt zijn met een onder buitenlandse beheer opererend netwerk (AS). Circa 54 procent van de Nederlandse 'Things' zijn gelinkt met vanuit de Verenigde Staten beheerde netwerken. Eén Amerikaans bedrijf alleen al is goed voor ruim 1,1 miljoen 'Things'. Nederland komt dan op de tweede plaats met 37 procent en ver daarachter volgen Zweden, het Verenigd Koninkrijk en Duitsland met respectievelijk 3, 3 en 2 procent. Als een apparaat gelinkt is aan een netwerk (AS) dat beheerd wordt vanuit een ander land wil dat niet zeggen dat de controle over het apparaat niet in handen is van de afnemer van de diensten van de desbetreffende Internet Service Provider. Maar het wil wel zeggen dat de zeggenschap over hoe het netwerk opereert in handen is van deze ISP en deze dus ook de mogelijkheid heeft om de dienstverlening stop te zetten.

Tabel 2. IoT: 'Things' fysiek aanwezig in Nederland naar land van 'Autonomous System', oktober 2017

Beherend land	Alle 'Things'		'Things' van overheid	
	abs.	%	abs.	%
Verenigde Staten	1 501 790	46,7	1 820	58,5
Nederland	1 204 265	37,4	650	20,9
Zweden	100 505	3,1	165	5,4
Verenigd Koninkrijk	88 015	2,7	110	3,5
Duitsland	68 585	2,1	55	1,8
Oostenrijk	63 565	2,0	20	0,7
Italië	49 560	1,5	105	3,4
Portugal	18 975	0,6	30	1,0
België	17 675	0,5	30	1,0
Vietnam	14 460	0,4	30	1,0
Zwitserland	13 430	0,4	25	0,9
Mexico	11 955	0,4	15	0,5
Frankrijk	11 795	0,4	15	0,5
Overige landen	52 130	1,6	40	1,3
Totaal	3 216 750	100,0	3 110	100,0

Bron: Censys.io, bewerking CBS

In de data waarmee gewerkt is, was ook informatie aanwezig over of een ‘Thing’ toegerekend kan worden aan een ‘government entity’. Het gaat daarbij om gemeenten, en andere overheidsinstellingen zoals universiteiten en ziekenhuizen. In totaal waren 3110 ‘Things’ op die manier te relateren aan de Nederlandse overheid. Dit waren allen servers.

Bij de interpretatie van de cijfers over fysieke locatie moet rekening worden gehouden met het feit dat veel websites tegenwoordig ook gebruikmaken van een zogeheten Content Delivery Network (CDN). Dit betekent dat de website gelinkt is met een grote Amerikaanse CDN waardoor het beheer administratief verschuift naar de Verenigde Staten terwijl de website technisch aanwezig kan zijn op een server in een ander land. CDN’s worden gebruikt om webcontent snel en efficiënt af te leveren bij eindgebruikers o.a. door kopieën van websites op te slaan zo dicht mogelijk bij eindgebruikers.

’Things’

In tabel 3 wordt een overzicht gegeven van de aantal apparaten die door Censys geregistreerd zijn. Na servers zijn ‘NAS’ en ‘Soho router’ de meest voorkomende apparaten die gemeten zijn. ‘NAS’ staat voor ‘Network Attached Storage’. Het betreft externe harde schijven die via een IP-adres data wereldwijd beschikbaar stellen voor gebruikers die toegang hebben tot deze NAS. ‘SOHO router’ staat voor ‘Small Office Home Office router’. Het gaat om breedband routers die gebruikt worden door kleine bedrijven om een Local Area Network (LAN) te bedienen. ‘Infrastructure routers’ worden vaker gebruikt bij grote bedrijven en Internet Service Providers om internetverkeer te sturen. Het voert te ver om hier alle apparaten uit tabel 3 van een toelichting te voorzien. Interessant is nog wel om te melden dat vooral ‘SCADA’ gerelateerde apparaten doorgaans veel aandacht krijgen vanuit cybersecurityperspectief. ‘SCADA’ staat voor ‘Supervisory Control And Data Acquisition). SCADA-systemen bieden de mogelijkheid om industriële machines te controleren zoals motoren, generatoren en fysieke sensoren. SCADA-geschikte apparaten worden veel gebruikt in de industrie, in fabrieken maar ook in energiecentrales en waterbehandelingsinstallaties. Aanvallen op deze systemen kunnen dramatische gevolgen hebben. Modbus is een van de belangrijkste protocollen bij SCADA. Dit protocol was oorspronkelijk ontwikkeld voor kleinschalige lokale communicatie maar is steeds meer ook in gebruik geraakt op grotere netwerken en het Internet.

Tabel 3. IoT: 'Things' naar type apparaat, oktober 2017

Type apparaat	Gelinkt met Nederlands AS	Fysiek aanwezig in Nederland
servers	1 304 950	3 140 245
nas	25 710	31 630
soho router	23 315	24 520
infrastructure router	5 595	5 595
network	5 330	3 285
IPMI	4 465	4 450
cable modem	1 860	1 930
camera	1 250	1 350
DSL/cable modem	1 235	1 310
firewall	510	565
printer	450	515
power distribution unit	440	440
DSL modem	390	390
scada controller	245	250
alarm system	80	95

switch	65	70
scada gateway	30	30
kvm	30	40
set-top box	20	25
programmable logic controller	10	10
solar panel	10	10
scada server	5	5
hvac	5	5
DVR	< 5	5
laser printer	< 5	< 5
environment monitor	< 5	5
scada router	< 5	< 5
Totaal	1 376 015	3 216 750

Bron: Censys.io, bewerking CBS

Het Modbus protocol vereist geen authenticatie; commando's die binnenkomen worden zonder controle op herkomst uitgevoerd. Ook is het bij veel SCADA-systemen nodig om met een user te werken met alle rechten ('admin' of 'root') wat inhoudt dat in geval zo'n systeem wordt gehackt de kwaadwillige partij volledige toegang krijgt tot zo'n SCADA-systeem.[5] Vanwege deze risico's is er veel aandacht van cybersecurity-specialisten voor deze problematiek. De data die beschikbaar komen via Censys bevatten informatie over de beveiligingspraktijken rond deze Modbus-apparaten. In het kader van dit artikel is deze informatie voor Nederland niet verder uitgezocht. Onderzoek van Censys wijst echter uit dat wereldwijd er ondanks de aandacht die het probleem heeft nog tal van Modbus-apparaten in verbinding staan met het Internet waarbij de veiligheidssituatie nog niet optimaal is. In tabel 3 is te zien dat er volgens Censys in Nederland 250 industriële systemen draaien waarbij gebruik wordt gemaakt van een SCADA-controler.

Met de groei van IoT nemen ook de kansen toe voor cybercriminelen om misbruik te maken van apparaten en servers. Er is daarom bij bedrijven en overheden veel aandacht voor het voorkomen en oplossen van kwetsbaarheden die aanwezig zijn in softwareproducten. In het vervolg van dit artikel wordt ingegaan op een aantal van deze kwetsbaarheden zoals die uit de analyse van de Censys-data over Nederland naar voren kwamen.

Kwetsbaarheden bij het HTTPS-protocol

Secure Sockets Layer (SSL) en Transport Layer Security (TLS) zijn veiligheidsprotocollen om websites te beveiligen. Om van SSL/TLS gebruik te kunnen maken moet een certificaat geïnstalleerd worden op de server dat SSL/TLS ondersteunt. Met behulp van een dergelijk certificaat en het HTTPS-protocol kunnen browsers en servers encryptie en authenticatie gebruiken om veilig te communiceren. Het HTTPS-verkeer gaat niet via poort 80 waarop het onbeveiligde HTTP-verkeer draait maar via poort 443. SSL is in 1995 geïntroduceerd door Netscape en werd wereldwijd de standaard voor het beveiligen van internetverkeer. In 1999 verscheen TLS als verbeterde versie van SSL 3.0. De eerste versies van SSL (1.0 en 2.0) bevatten een aantal kwetsbaarheden die aanvankelijk met versie 3.0 nog konden worden opgelost. Zo waren er bij SSL 2.0 problemen met de kwaliteit van de encryptie en de gebruikte algoritmen. Inmiddels wordt sinds 2015 ook het gebruik van SSL 3.0 afgeraden. TLS is daarmee de nieuwe veilige standaard geworden.

Servers die dus nog gebruikmaken van SSL 2.0 en/of SSL 3.0 lopen risico's. Uit de analyse van de Censys-data kwam naar voren dat medio oktober 2017 van de 525 duizend onder Nederlands beheer vallende servers die HTTPS-verkeer aanbieden nog bijna 170 duizend servers zijn waarop een van beide of beide versies geïnstalleerd is. Als we kijken naar de in Nederland aanwezig servers die HTTPS-verkeer aanbieden (1,608 miljoen) dan gaat het om ruim 210 duizend servers, waarvan slechts 46 bij een overheidsorganisatie.

In 2014 werd een fout ontdekt in 'OpenSSL', de opensource-software die gebruikmaakt van SSL/TLS. Het wordt gebruikt door alle grote besturingssytemen zoals Windows en Linux en applicaties zoals browsers. Kleine delen van het interne geheugen van een server konden onbedoeld worden uitgelezen waardoor in potentie ook sleutels, wachtwoorden en andere gevoelige gegevens niet goed beveiligd meer waren. Een nieuwe versie van het product (1.01.g) waarin het probleem was opgelost, werd op dezelfde dag beschikbaar gesteld. OpenSSL werd op dat moment veel gebruikt o.a. bij betalingen via iDEAL. Het lek kreeg de naam **'Heartbleed'** waarmee verwezen werd naar een klein onderdeel binnen de software (de heartbeat-extensie) dat het probleem veroorzaakte. De Censys-data tonen dat in oktober 2017 nog 1975 van de onder Nederlands beheer vallende servers gebruikmaken van de OpenSSL-versie die de fout bevat. Als we kijken naar de in Nederland aanwezige servers dan gaat het om 2505 servers, waarvan slechts één bij een overheidsorganisatie, een gemeente in Noord-Brabant.

In 2015 kwamen onder de naam **'FREAK attack'** nieuwe problemen aan het licht die gerelateerd waren aan HTTPS-verkeer. De problemen hadden te maken met een zwakke versleuteling die kon worden afgedwongen en ooit in de software was ingebouwd in de jaren negentig om de Amerikaanse inlichtingendienst NSA toegang te verschaffen tot versleuteld internetverkeer. Amerikaanse bedrijven mochten alleen softwareproducten naar het buitenland exporteren als daarin gebruik werd gemaakt van deze vorm van encryptie. Dit verbod was al lang opgeheven toen het probleem zich in 2015 aandiende. Het probleem kan worden opgelost door er voor te zorgen dat de server geen 'RSA-EXPORT cipher suites' accepteert. Een 'cipher suite' is een methode om het verkeer tussen een server en een client (browser) te versleutelen en te verwerken. Als een client zo'n versleutelde verbinding wil opzetten met een server, wordt aan de server gevraagd welke 'cipher suites' beschikbaar zijn. Vervolgens kiest de client de sterkste 'cipher suite'. Het gebruik van een aantal van deze cipher suites wordt inmiddels vanuit de beveiligingswereld afgeraden. Maar deze zijn vaak nog wel aanwezig op servers waardoor het omleiden en afluisteren van verkeer mogelijk is. In oktober accepteerden nog ruim 22 duizend van de onder Nederlands beheer vallende servers RSA-EXPORT cipher suites. Ruim 24 duizend van alle in Nederland aanwezige servers kenden deze kwetsbaarheid, waarvan drie bij een overheidsorganisatie (websites onder verantwoordelijkheid van een ministerie, een in Nederland gevestigd center of excellence van de NAVO en een provincie).

'Logjam Attack' is een ander encryptie-lek dat zich in 2015 openbaarde en sterke overeenkomsten heeft met 'FREAK attack' en het gerelateerde exportbeleid van de Amerikaanse overheid uit de jaren negentig. Bij dit lek doen zich problemen voor in zogeheten 'Diffie-Helmann sleuteluitwisseling' bij het opzetten van een versleutelde verbinding. Het algoritme is niet alleen essentieel voor het HTTPS protocol, maar o.a. ook voor SMTPS (mail) en SSH en protocollen die van TLS afhankelijk zijn. Alle mail- en webservers die 'Diffie-Hellman export encryptie' ondersteunen lopen risico's. In oktober accepteerden nog ruim 16 duizend van de onder Nederlands beheer vallende servers deze vorm van encryptie. Bijna 18 duizend van alle in Nederland aanwezige servers kenden deze kwetsbaarheid, waarvan slechts één bij een overheidsorganisatie (dezelfde website van een ministerie die ook kwetsbaar is voor 'Freak attack').

Tabel 4. IoT: Veilige en niet-veilige installaties van OpenSSH, oktober 2017

OpenSSH-versie	Op servers gelinkt met Nederlands AS	Op servers aanwezig in Nederland	Op servers aanwezig in Nederland in gebruik door een overheidsorganisatie
OpenSSH_5.3	51 505	58 275	< 5
OpenSSH_6.6.1p1	20 460	65 440	< 5
OpenSSH_6.7p1	20 385	31 390	< 5
OpenSSH_6.6.1	18 750	27 810	< 5
OpenSSH_7.2p2	17 625	72 600	-
OpenSSH_4.3	17 490	16 330	-
OpenSSH_6.0p1	13 065	18 475	< 5
OpenSSH_7.4	10 665	13 775	< 5
OpenSSH_7.4p1	4 545	7 820	-
OpenSSH_5.9p1	4 245	8 830	< 5
OpenSSH_5.5p1	3 610	4 935	-
OpenSSH_6.8p1-hpn14v6	3 310	4 045	-
OpenSSH_7.2	2 775	3 135	-
OpenSSH_6.6.1_hpn13v11	2 540	2 220	-
OpenSSH_6.6	1 790	1 625	-
OpenSSH_5.1p1	1 160	1 130	-
OpenSSH_7.3	1 155	1 405	-
OpenSSH_5.2	1 115	1 170	-
OpenSSH_7.5	1 110	1 415	-
OpenSSH_7.0	1 000	870	-

Bron: Censys.io, bewerking CBS

Dataencryptie

OpenSSH is een populaire opensource-implementatie van het SSH-protocol waarbij wachtwoorden en data met encryptie verstuurd kunnen worden om afluisteren, aanvallen en het ontsluiten van gevoelige informatie te voorkomen. Het draait op vrijwel alle besturingssystemen. Een versie van OpenSSH is aan te treffen op 214 duizend van de onder Nederlands beheer vallende servers en op ruim 363 duizend van de in Nederland aanwezige servers. In tabel 4 wordt een overzicht gegeven van de meest geïnstalleerde versies van OpenSSH. Te zien is dat voor de servers die gelinkt zijn met een Nederlands ‘Autonomous System’ met 51505 installaties versie 5.3 de meest voorkomende versie is. Deze versie dateert uit oktober 2009. De op een na meest recente versie 7.5 was een half jaar na verschijnen (maart 2017) nog maar aanwezig op 1770 servers. Het beeld voor de in Nederland aanwezige servers is enigszins anders. Versie 7.2p2 (maart 2016) is daar het meest geïnstalleerd met 72600 installaties.

De laatste jaren is gebleken dat ook binnen OpenSSH beveiligingsissues aan de orde zijn die alleen voorkomen kunnen worden met regelmatige updates. Een ernstig probleem werd manifest begin 2016 toen bleek dat de OpenSSH versies 5.4 tot en met 7.1 niet konden voorkomen dat vanaf andere 'kwaadwillende' of gehackte servers SSH-sleutels uitgelezen konden worden bij inlogprocedures. Het probleem bij deze versies is met een kleine ingreep in de server instellingen wel oplosbaar - door een ongedocumenteerde optie 'UseRoaming' op 'no' te zetten - maar het is niet waarschijnlijk dat dit op veel

servers is doorgevoerd. Het probleem verklaart mogelijk wel waarom in tabel 4 versie 7.2 nog redelijk hoog staat op de lijst van meest geïnstalleerde versies. De goede positie van versie 5.3 hangt hier waarschijnlijk ook mee samen. In oktober 2017 werkten nog 99015 servers die gelinkt zijn met een Nederlands 'Autonomous System' met een versie die kwetsbaar was voor dit probleem. Hoeveel servers daarvan alsnog de server hebben aangepast om het probleem te neutraliseren is niet bekend. Van alle in Nederland aanwezige servers werkten in oktober 2017 nog ruim 177 duizend servers met een kwetsbare versie. Het gebruik van OpenSSH bij overheidsorganisaties lijkt bijna niet voor te komen, zo is te zien in tabel 4.
Het is niet zomaar mogelijk om uitsluitend op basis van de geïnstalleerde versie van OpenSSH te constateren dat kwetsbaarheden aan de orde zijn. Het is namelijk ook mogelijk om op basis van 'patches' (software of bestanden die software kunnen updaten) kwetsbaarheden in OpenSSH-versies op te lossen. De versie blijft dan hetzelfde, maar het probleem wordt verholpen. Er is geen onderzoek gedaan naar het gebruik van patches door beheerders van servers.

Experimenteel onderzoek
Bij het onderzoek is gebruikgemaakt van een database met informatie over apparatuur die was aangesloten op ruim 150 miljoen IP-adressen wereldwijd. De kwaliteit van dit onderzoek is voor een belangrijk deel afhankelijk van de kwaliteit van de waarneming die is verricht door Censys. Er is door het CBS geen uitgebreid onderzoek gedaan naar deze kwaliteit. Zo is onduidelijk in hoeverre de aanduiding 'government entity' een volledig en correcte beschrijving geeft van dit domein. Ook is er aanleiding om nog beter in kaart te brengen hoe Censys de fysieke aanwezigheid van servers en andere apparaten registreert. Dit artikel betreft dus bovenal een verkenning van het onderwerp en de bron en de uitkomsten wil het CBS daarom ook kwalificeren als experimenteel. Er zijn echter geen redenen om op voorhand te twijfelen aan de kwaliteit van Censys mede gezien de historie die de organisatie heeft en de banden met de universitaire wereld. De data van Censys is nog niet lang niet volledig benut.

Het onderzoek is een voorbeeld van de wijze waarop het CBS bezig is om binnen het Center for Big Data Statistics (CBDS) op basis van nieuwe big data bronnen nieuwe statistieken te maken. De bevindingen nu al en de mogelijkheden die verder onderzoek van de data nog zullen bieden zijn dermate interessant dat het CBS de mogelijkheden zal verkennen om in de nabije toekomst met hulp van andere partijen dit onderzoek te continueren en te verdiepen. Verdieping van het onderzoek kan o.a. plaatsvinden door de monitoring (bijvoorbeeld maandelijks) van ontwikkelingen en ook door de positie en prestaties van Nederland ten opzichte van andere landen te onderzoeken. Ook kunnen door het koppelen van deze data met andere data waarover het CBS beschikt nog analyses per bedrijfsgroep worden gedaan.

---

[1] Bron: OECD Digital Economy Outlook 2015.

[2] De twee gekozen invalshoeken (vallend onder beheer van een Nederlands AS of Nederland als locatie van de apparaten) geven nog geen volledig beeld. Om een goed overzicht te krijgen van het IoT van Nederlandse bedrijven is ook nog informatie nodig waarmee IP-adressen aan Nederlandse bedrijven gekoppeld kunnen worden. Het CBS werkt wel aan een dergelijk register, maar momenteel is dit nog niet gereed. Ter illustratie: een in dit artikel geteld apparaat hoeft niet per se van een Nederlands bedrijf te zijn. Het kan bijvoorbeeld ook gaan om een apparaat dat door een Zweeds bedrijf via een Nederlandse ISP aan het Internet is verbonden. Eveneens zitten bijvoorbeeld niet in de telling servers die een Nederlands bedrijf via een buitenlandse ISP gebruikt en zich niet in een datacentrum in Nederland bevinden.

[3] Op het concept 'Internet of Things' en verschillende definities wordt uitgebreid ingegaan in een publicatie van IEEE: 'Towards a definition of the Internet of Things (IoT)' uit mei 2015.

[4] Uitgebreide informatie over Censys is te vinden in het volgende artikel van de makers van Censys: Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey en J. Alex Halderman, A Search Engine Backed by {I}nternet-Wide Scanning, in Proceedings of the 22nd ACM Conference on Computer and Communications Security, oktober 2015.

[5] Bron: Cyber-security of SCADA and Other Industrial Control System, Edward J.M. Colbert en Alexander Kott, Springer 2016.