iB
INFORMATIEBEVEILIGING
jaargang 15 - 2015
#8

UNSAFE HARBOUR

Na de veilige haven

Interview iWelcome: Danny de Vreeze en Maarten Stultjens

Extreme Weather Events

Meldplicht datalekken

Gezocht: IT security trainees!

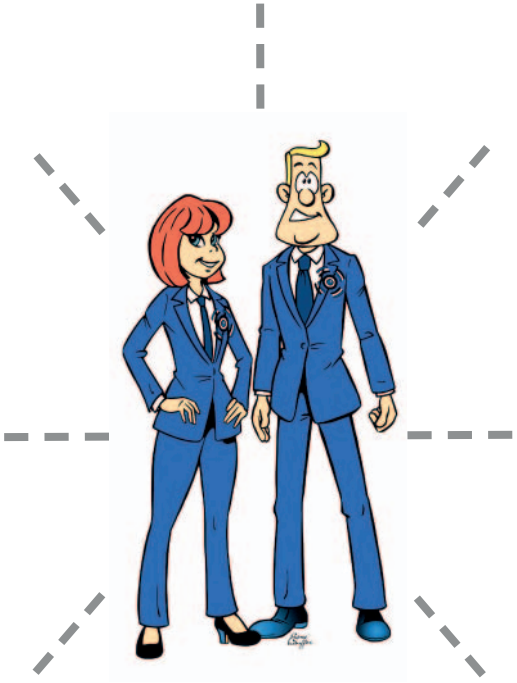
Start begin 2016

"Realiseren van veilige innovatieve IT-infrastructuren."

SecureLink is opgericht in **2003** en heeft **200** enthousiaste SecureLinkers. We hebben **4** vestigingen verdeeld over Nederland en België.

Detail • Klantgerichtheid • Respect • Commitment • Bezieling • Creativiteit • Enthousiasme

Het hoofdkantoor van SecureLink bevindt zich in Sliedrecht (regio Rotterdam). Jouw werkgebied ligt vooral in de Randstad, maar ook de rest van Nederland.



"Breed beginnen en daarna specialiseren in de richting van jouw keuze."

"Naar hartenlust experimenteren in een lab met state-of-the-art apparatuur."

Best Workplaces – Great Place To Work – Securelink Nederland B.V.

fd. Gazellen Awards 2011 - 2014

Deloitte. Technology Fast 500

Secure UNIVERSITY

Trainees worden binnen één jaar klaargestoomd voor de functie van Security Specialist!

Een greep uit onze klanten

bol.com, vpro, HU Hogeschool Utrecht, BNN VARA, Mitsubishi, Zi

Interesse in deze vacature?
Neem contact op met Tim Boerakker via T +31 88 1234 200 of mail naar jobs@securelink.nl.
Kijk voor meer informatie op www.securelink.nl.

Go Secure!

DE ZWAKSTE SCHAKEL

In de kern willen we dat cloudleveranciers die onze data verwerken ook in ons belang handelen. Wanneer nodig. Eigenlijk altijd. Dat is het hoogste niveau van vertrouwen dat je kunt hebben, en levert ook het meeste toegevoegde waarde voor een bepaalde inzet.

Dit valt echter in een wereld van politieke spelers die elkaar door-en-door wantrouwen. In de politiek vertrouwen we elkaar niet, we maken afspraken en eenieder beloont de ander voor het zich houden aan de afspraak en straft als het tegendeel aan het licht komt. Tegelijkertijd proberen we zelf waar mogelijk onder afspraken uit te komen. Dit is zo ongeveer het laagste niveau van vertrouwen dat je kunt hebben. Toegevoegde waarde kan er nog steeds zijn, maar het is wel minder.

Beide kunnen technisch veilig uitgevoerd worden. Een hoog niveau van vertrouwen is eenvoudig ingericht. Een laag niveau vraagt om maatregelen en controles. Vandaar die lagere opbrengst.

Nu zie je dat veel clouddiensten hun toegevoegde waarde berekenen aan de hand van een hoog niveau van vertrouwen. Want ze zijn toch te vertrouwen? Extra maatregelen zijn niet nodig. 'Don't be Evil'... Laten we er even van uitgaan dat dit zo is. Dan nog is de leverancier van deze diensten in een land gevestigd. En slaat zijn data op in een (ander) land. En verwerkt die data weer in een ander land. En in ieder van die landen kan de clouddienst aangesproken worden op juridische (lees: politieke) verplichtingen.

Je begrijpt wel waar ik heen wil: kun je als Europese klant een clouddienst vertrouwen in zo'n meervoudige politieke omgeving? En mag je dit? Die laatste vraag is vooral van belang voor onderdelen van de overheid zelf. Ik kom tot de conclusie dat vertrouwen een keten is: zo sterk als de zwakste schakel. En die zwakste schakel is politiek gezien per definitie een ander. Zo komen we aan verdragen als Safe Harbour.

Nog erger wordt het als die veilige uitvoering waar ik het eerder over had politiek niet toegestaan wordt. Als sterke encryptie afgezwakt moet worden met een achterdeur, dan zijn we op dat moment hard bezig die zwakste schakel nóg verder af te vijlen.

In dit nummer

NA DE VEILIGE HAVEN

Gegevens uitwisselen na Schrems vs. Facebook

Safe Harbour is niet meer. Op 6 oktober 2015 deed het Europees Hof van Justitie een baanbrekende uitspraak in de zaak Schrems vs Facebook: Safe Harbour is ongeldig en kan dus niet meer gebruikt worden als basis om gegevens uit te wisselen tussen de EU en de USA. Ook mogen Data Protection Agencies (DPAs) onderzoek doen naar buitenlandse bedrijven die gegevens verwerken van EU onderdanen als er een vermoeden is dat inbreuk wordt gemaakt op Europese privacywetten. Twee conclusies met grote impact. Maar, wat ging daaraan vooraf? En, belangrijker nog: wat moet je als bedrijf of organisatie doen als je op dit moment zaken wil gaan doen met een Amerikaans bedrijf?

Nul op het rekest bij de privacytoezichthouder

Max Schrems, een Oostenrijkse privacyactivist, had bij de Ierse toezichthouder een klacht ingediend tegen Facebook omdat zijn gegevens van Ierland naar Amerika worden verzonden. Volgens hem een inbreuk op zijn privacy. Na de onthullingen van Snowden over PRISM en de massasurveillance van de NSA zouden zijn gegevens niet veilig zijn in de Verenigde Staten. De Ierse toezichthouder wees de klacht van Schrems af en weigerde onderzoek te doen naar Facebook. Zij heeft geen verplichting om op te treden oordeelde ze want de uitwisseling van gegevens is rechtmatig. De voorzitter van de Ierse DPA wees naar het bestaan van Safe Harbour en stelde daarover in een interview dat "Irish law faithfully transposes European law in this area, it lays down very clearly that once there's been a decision that data can flow to different countries, then I am bound by that decision and that is why there is nothing to investigate by me in this case" [1].
Schrems vecht de beslissing aan bij de Ierse High Court. Het Ierse High Court oordeelt dat de Europese privacywetgeving geldt boven de Ierse privacywetgeving en dat daarom de zaak beoordeeld dient te worden naar Europees privacyrecht [2]. De Ierse High Court doet nog geen uitspraak en houdt de zaak aan; zij wil eerst prejudiciële vragen voorleggen aan het EU Hof van Justitie (HvJ EU) over de uitleg van Europese privacywetgeving in het licht van de klacht van Schrems. Alleen het HvJ mag namelijk uitleg geven over de toepasselijkheid en reikwijdte van de Europese privacyregels.

Kritische evaluaties Safe Harbour

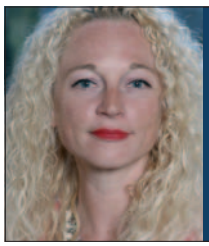
De uitspraak van het HvJ [3] is het sluitstuk in een langlopende strijd over Safe Harbour en de vraag naar de effectiviteit van het middel. In 2002 (EU) [4], 2004 (EU) [5] en 2008 (Galexeia) [6] vinden er externe evaluaties plaats van Safe Harbour. In alle drie de evaluaties is kritiek op compliance met en handhaving van de privacyregels. Zo bleek uit de studie in 2008 (Galexeia) onder meer dat:

- Er 1597 organisaties op de Safe Harbour-lijst stonden, maar dat slechts 1109 organisaties lid waren van Safe Harbour.
- Slechts 348 van die organisaties voldoen aan (enkele van) de basisvereisten van Safe Harbour.

Ook binnen de Europese Unie zelf is er kritiek over de effectiviteit van het framework. In de externe evaluatie van 2004 stelt de Europese Commissie dat het Amerikaanse Department of Commerce actiever dient te gaan handhaven. Ook blijkt uit de evaluatie dat een groot deel van de gecertificeerde bedrijven niet voldoet aan de basisvereisten van Safe Harbour. In 2013 schrijft de Commissie: "There has been a growing concern among some data protection authorities in the EU about data transfers under the current Safe Harbour scheme. Some Member States' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by industry, referring to distortions of competition due to a lack of enforcement" [7]. in 2013, het jaar van de Snowden-onthullingen, geeft de Commissie in diezelfde communicatie ook aanleiding om kritiek te uiten over massasurveillance: "Furthermore, the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the US." Safe Harbour voorziet in een clausule waardoor het toegestaan is in het kader van nationale veiligheid inbreuk te maken op de privacy van EU onderdanen, echter in de 2013-communicatie geeft de Commissie aan dat deze uitzondering slechts zeer beperkt mag worden ingezet: "It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate." De Commissie doet 13 aanbevelingen voor verbeteringen waaraan moet worden voldaan om Safe Harbour weer "safe" te maken. In de zomer van 2014 verloopt de deadline daarvoor, de aanbevelingen zijn nog niet allemaal opgevolgd. Vanuit de EU laat Commissaris Viviane Reding weten dat de "national security exception" het grote struikelblok is in de onderhandelingen, de Amerikanen stellen: "we have reached agreement on many of the issues" [8].

De uitspraak van het HvJ

Terwijl de onderhandelingen tussen de EU en de USA over vernieuwing van Safe Harbour moeizaam verlopen, staat de legaliteit van de afspraak op de gerechtelijke agenda door de pre-judiciële vragen van het Ierse High Court. Eind september 2015 geeft Advocaat-Generaal Bot zijn conclusie in die zaak en stelt dat Safe Harbour ongeldig is [9]. In de uiteindelijke uitspraak van het HvJ op 6 oktober wordt vele malen naar zijn conclusie en de argumentatie daarin verwezen. Het Hof komt tot haar ongeldigheidsoordeel op grond van meerdere (samenwerkende)



Mr Rachel Marbus is Privacy Officer NS en bestuurslid van het PvIB. Zij is bereikbaar via rachelmarbus@gmail.com.

redenen. Zo oordeelt het Hof dat:

1. Safe Harbour niet voorziet in een goede procesgang voor personen die zich benadeeld zien.
2. Er geen mogelijkheid bestaat voor personen om toegang te krijgen tot hun persoonsgegevens en om deze te laten wijzigen of wissen.
3. Safe Harbour verhindert Data Protection Agencies om onderzoek te doen naar privacyinbreuken door Amerikaanse bedrijven.

In een persbericht benadrukt het Hof dat onderzoek naar privacyinbreuken altijd mogelijk moet zijn: "Thus, even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive" [10]. Ook neemt het Hof stelling over de vraag naar de toelaatbaarheid van massasurveillance door de Amerikaanse overheid. Naar het oordeel van het Hof is de surveillance te breed en ongericht en vormt het daardoor een inbreuk op de privacy van personen: "the Court finds that, under EU law, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use."

En wat nu?

Na de uitspraak van het Hof gaan de onderhandelingen over nieuwe afspraken tussen de EU en de USA onverminderd door. De voorzitters van de DPAs van de EU, verenigd in de artikel 29 werkgroep, hebben aangegeven dat zij verwachten dat er in januari 2016 nieuwe afspraken liggen. Mochten die afspraken in januari niet gereed zijn, dan zullen de DPAs handhavend gaan optreden tegen Amerikaanse bedrijven: "EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions" [11]. In hetzelfde persbericht geven de DPAs ook aan dat er in de tussenliggende periode twee middelen zijn die verantwoordelijken nu nog ter beschikking staan. De EU Model Clauses en de Binding Corporate Rules.

De Model Clauses zijn opgesteld door de Europese Commissie. Het is een standaardcontract waarin privacyregels voor gegevensuitwisselingen worden afgesproken. Dit modelcontract kan rechtstreeks van de site van de Commissie gehaald worden [12]. Er is weinig ruimte voor afwijking van de voorwaarden zoals die zijn vastgelegd in het model. Er mag meer worden afgesproken, maar zeker niet minder. Mocht er toch aanleiding zijn om wijzigingen in het standaardcontract aan te brengen, dan kan dat betekenen dat nog een gang naar het College Bescherming Persoonsgegevens nodig is om de wijziging goedgekeurd te krijgen. De Model Clauses worden namelijk (in beginsel) alleen geaccepteerd als deze ongewijzigd worden overeengekomen. Daarnaast kan gedacht worden aan het maken van afspraken met bedrijven waarin vastgelegd wordt dat persoonsgegevens niet verwerkt zullen worden buiten de Europese Unie. Steeds vaker bieden Amerikaanse bedrijven een "EU-oplossing" aan door te garanderen dat data in datacenters binnen de EU-grenzen blijft. Let wel, je bent daarmee niet gegarandeerd gevrijwaard van dataopvragingen door de Amerikaanse overheid. Er bestaan nog steeds mogelijkheden voor de Amerikaanse overheid om gegevens op te vragen ook al staan deze op EU-grondgebied. Momenteel loopt er nog een rechtszaak tussen Microsoft en de Amerikaanse overheid om juist dit aspect aan te vechten [13]. Een tweede optie is het gebruik van Binding Corporate Rules (BCR). BCR is een juridisch middel wat ingezet kan worden om gegevensuitwisseling binnen een internationaal bedrijf mogelijk te

De tijdslijn Schrems vs Facebook

26. 6. 2013
Klacht ingediend bij de Ierse toezichthouder tegen "Facebook Ireland" vanwege het doorgeven van gegevens aan USA.

25. 7. 2013
Ierse toezichthouder vindt dat er geen plicht bestaat om onderzoek te doen, ze stelt dat de klacht "frivolous and vexatious" is.

24. 10. 2013
Er wordt een rechtszaak begonnen tegen het oordeel van de Ierse toezichthouder (Irish High Court).

18. 6. 2014
Irish High Court stelt pre-judiciële vragen aan Europees Hof van Justitie.

24. 3. 2015
Zaak komt voor Eu HvJ.

23. 9. 2015
Advocaat-Generaal Bot brengt zijn oordeel uit (zeer negatief over Safe Harbour). Vaak wordt het oordeel van de AG overgenomen door het HvJ, zij zijn daartoe echter niet verplicht.

6. 10. 2015
EU HvJ doet uitspraak: Safe Harbour is ongeldig en lokale Data Protection Agencies hebben het recht onderzoek te doen naar buitenlandse entiteiten die mogelijk EU privacywetten overtreden.

BCR: Binding Corporate Rules, privacyregels die afgesproken worden voor 1 bedrijf. Binnen dat hele bedrijf en al haar internationale vestigingen worden deze regels nageleefd, zijn aan goedkeuring van de toezichthouder onderhevig.

Europees Hof van Justitie: hoogste gerecht binnen de Europese Unie, doet uitspraken over het toepassen van EU recht (doet bindende uitspraken over hoe het recht geïnterpreteerd moet worden en moet zorg dragen voor uniforme toepassing binnen de EU).

EU MC: Model Clauses (modelcontract) van de Europese Unie die regels vastleggen waaronder uitwisselen van persoonsgegevens met landen waar geen adequate bescherming van de privacy is, geoorloofd is.

Pre-Judiciële vragen: een rechtsvraag van een rechter aan een hoger gerecht over de uitleg van een rechtsregel. Hangende de behandeling van die vraag bij de hogere rechter, wordt de procedure voor de lagere rechter geschorst. De lagere rechter zal na de prejudiciële uitspraak zelf ook uitspraak doen met toepassing van de prejudiciële uitspraak.

maken. In de BCR worden zeer nauwgezet de privacyregels vastgelegd waaraan een bedrijf zich zal houden. Vaak zal dit vrij dicht aansluiten bij het bestaande Europese privacyrecht. De BCR kan vervolgens aan de privacytoezichthouder (CBP) worden voorgelegd ter goedkeuring. Daarmee verkrijgt het een officiële status en kan binnen het hele bedrijf gegevensuitwisseling plaatsvinden. Let wel, met die officiële status zullen de BCR ook direct een document worden op grond waarvan de toezichthouder handhaaft.
Op het moment van schrijven wordt nog steeds onderhandeld over nieuwe afspraken. In een toespraak heeft Commissaris Jourová echter al wel laten weten dat afspraken gemaakt zullen worden over sterker pro-actief toezicht met sancties bij niet naleven [14]. Daarnaast wordt gewerkt aan afspraken waarin de DPA's een rol zullen krijgen binnen het nieuwe Safe Harbour. Zij worden betrokken in de jaarlijkse evaluaties van Safe Harbour 2.0.

Referenties

[1] Infosecurity-magazine.com, Facebook: Irish Regulator to Face Judicial Review Over Refusal to Consider PRISM, 26 oktober 2013 <http://www.infosecurity-magazine.com/news/facebook-irish-regulator-to-face-judicial-review/>
[2] Irish High Court, Maximilian Schrems vs Data Protection Commissioner, judgement 18th June 2014, 2013 no. 765JR.
[3] Judgement of the Court, 6 October 2015, In Case C?362/14, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximillian Schrems v Data Protection Commissioner
[4] European Commission (2002) The application of Commission Decision on the adequate protection of personal data provided by the Safe Harbour Privacy Principles, Brussels, 13-02-2002 SEC(2002) 196
[5] European Commission (2004) The implementation of Commission Decision on the adequate protection of personal data provided by the Safe Harbour Privacy Principles, Brussels, 20-10-2004 SEC (2004) 1323
[6] Chris Connolly (Galexia) US Safe Harbor - Fact or Fiction? Privacy Laws and Business International, issue 96, December 2008, published on Galexia.com
[7] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM 2013/847
[8] Stephen Garder, Bloomberg, Progress Slow on Talks Over Revision Of U.S.-EU Safe Harbor, Officials Say, 24 November 2014, < http://www.bna.com/progress-slow-talks-n17179912506/>
[9] Opionion of Advocate General Bot delivered on 23 September 2015 (1) Case C?362/14, Maximillian Schrems v Data Protection Commissioner, (Request for a preliminary ruling from the High Court (Ireland))
[10] Court of Justice of the European Union, Press Release No 117/15, Luxembourg, 6 October 2015, Judgment in Case C-362/14 Press Maximillian Schrems v Data Protection Commissioner
[11] Article 29 Data Protection Working Party - STATEMENT on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), 16-10-2015
[12] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
[13] The Guardian, Microsoft case: DoJ says it can demand every email from any US-based provider, 9 September 2015, <http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant>
[14] Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe), Strasbourg, 26 October 2015, Speech by Commissioner Jourová before the Committee on Civil Liberties, Justice and Home Affairs (Libe)

Maarten Stultjens

WELKOM IN DE WERELD VAN CLOUD IAM

Identity & Access Management (IAM) is hot. Was het enkele jaren geleden nog 'IT-hygiëne' (iets dat je op orde moest hebben), anno nu is IAM in de woorden van Danny de Vreeze en Maarten Stultjens van iWelcome met name ook een 'business enabler'. Een randvoorwaarde voor elk bedrijf dat een digitale relatie wil opbouwen met klanten. Tijd dus om kennis te maken met iWelcome in Amersfoort. Dit in het kader van de artikelreeks waarin Informatiebeveiliging een kijkje in de keuken krijgt van succesvolle innovatieve bedrijven in de branche.

In deze series interviews presenteert IB opvallende en innovatieve Nederlandse security bedrijven en gaat op zoek naar wat hen drijft en bezighoudt en welk probleem zij willen oplossen.

Danny de Vreeze

Dat iWelcome hiertoe behoort, blijkt bijvoorbeeld uit het feit dat het bedrijf door Gartner in het Magic Quadrant wordt gezien als de enige 'established' Europese leverancier van IDaaS (Identity en Access Management as-a-Service). Maar ook uit de certificering van de Nederlandse overheid van iWelcome's eHerkenningsmakelaar waarmee bedrijven op een betrouwbare manier digitaal zaken kunnen doen met de Nederlandse overheid. We spreken met CEO Danny de Vreeze en Maarten Stultjens, binnen iWelcome verantwoordelijk voor Sales en Business Development.

'Angstdiscussie ligt in het verleden'

De genoemde erkenningen maken beide heren natuurlijk trots. Maar verbaasd erover zijn ze nu ook weer niet. Danny de Vreeze zag in 2011 met inmiddels vijftien jaar IAM-ervaring de opkomst van de cloud al als een kans voor nieuwe businessmodellen op zijn vakgebied. En deze kans heeft hij gegrepen. Door bij de oprichting van iWelcome dus direct al te kiezen voor IAM in de cloud.

Een veiligheidsrisico? Deze angstdiscussie ligt volgens De Vreeze anno 2015 echt in het verleden. "Alles gebeurt al in de cloud, steeds meer enterprises kiezen voor de volledige go-to-cloud-strategie. Hier hoort IAM in de cloud dus ook bij."

En dus heeft iWelcome een eigen IDaaS-platform ontwikkeld voor enterprises gebaseerd op open standaarden en gebouwd met gerenommeerde open source componenten dat voldoet aan de hoogste beveiligingsstandaarden.

"Daarbij hebben wij expliciet voor de cloud gekozen omdat klanten onze certificering en processen gebruiken in hun compliancy vereisten. Daarvoor moeten wij wel in control zijn. En dat kan alleen als het in onze omgeving gebeurt en die staat in onze datacenters onder onze control."

De Vreeze: "Met onze IDaaS-implementatie bij PostNL laten we bijvoorbeeld zien dat we zestigduizend gebruikers veilige en flexibele toegang kunnen bieden tot tientallen applicaties. Datzelfde geldt voor onze IDaaS-oplossing bij NXP die is

Sandra Kagie is freelance tekstschrijver/journalist (website: www.sanscriptproducties.nl; twitter@SanSanscript). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'.

‘De basis van identity management vormt de juiste balans in waarde/moeite-perceptie’

verbonden met het on-premise IAM-systeem en die tal van (cloud)applicaties voor meer dan drie-en-twintig duizend gebruikers over de hele wereld ontsluit.”
Twee projecten waarvoor het bedrijf dit jaar en vorig jaar werd onderscheiden op de jaarlijkse European Identity Conference (zie het kader voor meer informatie hierover).

De rode loper

De Vreeze ziet het IDaaS-platform van iWelcome als de rode loper die leidt naar het virtuele kantoor. Een rode loper waarop je wanneer je een uitnodiging hebt welkom bent. Heb je deze uitnodiging echter niet dan word je onherroepelijk van de rode loper verwijderd.
“Dankzij een mix van technologieën, proberen wij bezoekers van een website of gebruikers van een applicatie zich zo welkom mogelijk te laten voelen. We monitoren 24/7, maar we zijn zo lang mogelijk onzichtbaar. Zoals je je als kijker naar de rode loper van de Oscar-uitreiking ook niet bewust bent van de vele security-maatregelen die er getroffen zijn”, legt hij uit.

Maarten Stultjens geeft vervolgens het voorbeeld van een onderwijsinstelling. “Gebruikers van applicaties, in dit geval leerlingen en docenten, zijn het meest gebaat bij gebruiksgemak. Je wilt hen als gebruiker een Single Sign-On bieden”, legt hij uit. Zodat ze na een eenmalige aanmelding vanaf ieder apparaat en op elk moment toegang kunnen krijgen tot de voor hen benodigde applicaties en informatie, zowel in de cloud als on-premise.
“Wanneer het echter aankomt op bijvoorbeeld cijfers en beoordelingen van leerlingen dan is een hogere mate van zekerheid dat een gebruiker bij deze informatie mag komen noodzakelijk. En precies in dit speelveld bewegen we ons. We maken samen met opdrachtgevers de continue afweging hoe gemakkelijk een bepaalde applicatie en daarmee informatie voor een gebruiker toegankelijk moet of mag zijn.”

Waarde/moeite-perceptie

“De basis van identity management binnen consumentgericht IAM vormt de juiste balans in waarde/moeite-perceptie”, gaat De Vreeze verder. “Maak je het gebruikers/bezoekers te snel te moeilijk dan haken ze heel snel af. Maar werp je helemaal geen barrières op voor toegang tot gevoelige gegevens dan kom je in de krant. Tussen ‘open’ en ‘dicht’ in termen van identity management zitten diverse levels. Het iWelcome-platform is erop ingericht om al deze niveaus en afwisseling daarin te ondersteunen.”
Een ontdekkingstocht die volgens beide heren voor organisaties steeds complexer wordt. Omdat grenzen in de wereld van de informatietechnologie anno 2015 meer en meer vervagen. Denk aan de toenemende acceptatie van cloudapplicaties, de gewenste toegang voor externe gebruikers (guest-users) en van ongecontroleerde apparaten, ook wel Bring Your Own Device of BYOD genoemd.
En ontwikkelingen gaan nog verder. Zo wijst De Vreeze op de wens van veel gebruikers om in te kunnen loggen op online diensten en/of applicaties met een Facebook-, LinkedIn- of Google-profiel om zo de eigen identiteit te authenticeren. Bring Your Own Identity, ook wel BYOI of BYOID genoemd. De ‘consumerization’ van authenticatietechnologie waar bedrijven en organisaties anno nu volgens hem op voorbereid moeten zijn. “Ingewikkeld en duur wanneer je als organisatie blijft vasthouden aan een traditioneel, on-premise, IAM-systeem en zelf deze ontwikkeling moet blijven bekostigen.”

Band opbouwen vanuit digitale relatie

IDaaS staat door de genoemde ontwikkelingen volgens Stultjens aan de basis van de huidige transformatie die vooral veel business-to-consumer bedrijven en organisaties momenteel doormaken. “Deze bedrijven moeten meer en meer interacteren met klanten. Om zo een band op te bouwen vanuit een digitale relatie”, licht Stultjens toe. En hij noemt vervolgens voorbeelden van ontwikkelingen als e-learning, maar ook zorg op afstand en de slimme meters die veel energiebedrijven introduceren. Het aantal contactmomenten dat bedrijven en organisaties met consumenten hebben gaat omhoog en contact wordt veel meer tijd- en plaatsonafhankelijk. Een ontwikkeling die volgens hem vraagt om robuust identity management.
“Naarmate de waarde van een dienst toeneemt, wil je als bedrijf of organisatie immers zeker weten dat je daadwerkelijk te maken hebt met de persoon waarmee je denkt te maken te hebben. Steeds weer dit stukje zekerheid en vertrouwen bieden, is onze rol in het geheel.”

Private-tenant-platform

iWelcome biedt enterprises, overheden, zorg- en onderwijsinstellingen dus een honderd procent Europese Identity-as-a-service-dienst. Het is hierbij voor De Vreeze vanaf de start in 2011 de bedoeling geweest opdrachtgevers een private-tenant-platform te bieden. “Iedere opdrachtgever

Best Cloud Security Project

Dit jaar en vorig jaar won iWelcome op de jaarlijkse European Identity Conference de prijs voor 'Best Cloud Security Project Europe'. In 2014 voor het IDaaS-project bij NXP en dit jaar voor het project bij PostNL. Uitreikingen waarbij de jury in beide gevallen benadrukte dat het IDaaS-platform van iWelcome snel aan te sluiten is (denk hierbij aan een traject van drie maanden) en dat het bovendien een honderd procent Europese oplossing betreft. Belangrijk voor veel Europese enterprises, want hun data blijft met iWelcome dus gegarandeerd in Europa. Het bedrijf valt namelijk als enige Cloud IAM-leverancier onder de Europese wet- en regelgeving en niet onder de US Patriot Act.

No more Safe Harbour

Een claim die Maarten Stultjens namens iWelcome onderstreept door een uitstapje te maken naar de uitspraak van het Europese Hof van Justitie medio oktober waarmee het Safe Harbour-verdrag ongeldig is verklaard. Het privacyverdrag tussen de Verenigde Staten en Europa. Amerikaanse bedrijven kunnen hierdoor niet langer op grond van Safe Harbour garanderen dat gegevens van Europese burgers en bedrijven voldoende beschermd zijn. Een test op de Safe Harbour-checker van Tresorit maakt de gevolgen van deze uitspraak direct duidelijk. Je kunt hier namelijk controleren of bedrijven waarmee je zaken doet persoonlijke gegevens uitwisselen met de Verenigde Staten. Tik je hier de bedrijfsnaam 'iWelcome' in dan krijg je een veilig 'groen' scherm. Doe je hetzelfde met bijvoorbeeld 'Microsoft' dan krijg je een onveilig 'rood' scherm met daarbij de waarschuwing: 'Using their service for processing personal data might be risky'.

beschikt dus over een gescheiden omgeving", legt hij uit. "Zodat we iedereen voldoende flexibiliteit kunnen bieden om zo aan te kunnen sluiten bij het ritme van de klant", gaat hij verder. "Zo zit niet elke opdrachtgever op hetzelfde moment te wachten op een update van een missiekritieke infrastructuurcomponent als IAM. Door met deze gescheiden omgevingen te werken, kunnen we updates echter volledig afstemmen op de bedrijfsprocessen van de klant."
Maatwerk gaat wat De Vreeze en Stultjens betreft te ver. "Maar we kunnen met onze IDaaS-dienst absoluut meebewegen met opdrachtgevers", geven ze aan. Daarbij is een belangrijke eigenschap van de IDaaS-oplossing van iWelcome dat deze gericht is op elk type gebruiker. Dus niet alleen op medewerkers, waar veel traditionele IAM-systemen op zijn gericht, maar ook op consumenten, toeleveranciers en gastgebruikers. "We willen met onze oplossing het complete identity-vraagstuk van opdrachtgevers tackelen", benadrukt De Vreeze. "En hen daarbij nadrukkelijk de mogelijkheden laten zien van nieuwe businessopportunities die gedegen identity management met zich meebrengt", vult Stultjens aan.

Want dat het vakgebied van identity management nog lang niet is uitontwikkeld, daarvan zijn beide heren overtuigd. "De markt gaat exploderen", voorspelt De Vreeze. "Voorbeelden van dienstverlening waar één of andere vorm van elektronische identiteit en authenticatie op de achtergrond een onmisbare rol speelt, nemen nog elke dag toe. Zorg er als bedrijf of organisatie dus voor dat je de rode loper uitlegt. Maar dat je alleen mensen mét een uitnodiging toelaat", waarschuwt hij.
Alleen op deze manier kun je volgens hem als bedrijf de stap succesvol maken van de traditionele 'fysieke' wereld waarin persoonlijk contact centraal stond naar de digitale wereld waarin digitaal contact aan de basis staat van vrijwel elke relatie.

EXTREME WEATHER EVENTS

Benaderd vanuit MKB-accountancy

Het wereldwijde klimaat en ook het klimaat in Nederland gaat veranderen en veroorzaakt waarschijnlijk meer weerextremen in de vorm van stormen, hevige regenbuien en hittegolven. Met de groei van data en netwerken en de steeds groter wordende afhankelijkheid die bedrijven, overheden en consumenten van ICT hebben, wordt het duidelijk dat ICT-diensten zoals telefonie, datacommunicatie en internet continu beschikbaar moeten zijn en in het geval van een calamiteit zo snel mogelijk weer hersteld. Er is al veel onderzoek gedaan naar de vitale infrastructuur in Nederland maar in welke mate zijn MKB-accountancybedrijven voorbereid op mogelijk uitval van ICT door Extreme Weather Events?

Het onderzoek

Het wereldwijde klimaat en ook het klimaat in Nederland gaat volgens internationale weerdeskundigen veranderen en veroorzaakt in toenemende mate meer weerextremen in de vorm van stormen, hevige regenbuien en hittegolven. Doordat de temperatuur stijgt komen zachte winters en hete zomers vaker voor en neemt (extreme) neerslag in de winter en zomer toe. Daarnaast neemt het tempo van de zeespiegelstijging toe. Om de schadelijke gevolgen hiervan op de maatschappij te voorkomen of te beperken is aanpassing op het klimaat nodig. Welke maatregelen moeten we treffen om de nadelige effecten van klimaatverandering te voorkomen of te beperken? Eerder is al onderzoek gedaan naar effecten van weersextremen betreffende de vitale infrastructuren van Nederland, echter niet naar de effecten op het MKB. Vooral bij dienstverlenende bedrijven binnen het MKB maakt vrijwel iedereen gebruik van ICT en neemt de afhankelijkheid hiervan alleen maar toe. Het MKB vormt als groep een belangrijk onderdeel van de economie van ons land. In Nederland is 66,9% van de beroepsbevolking werkzaam bij MKB-bedrijven en heeft een aandeel van 64,2% in het Bruto Nationaal Product. De kans van optreden en de effecten van weersextremen op uitval van ICT zijn moeilijk te voorspellen, wel kan worden onderzocht in hoeverre voorbereidingen zijn getroffen om uitval van ICT te voorkomen en wat de mogelijke impact van uitval is. Dit onderzoek heeft zich gericht op de mate van voorbereiding en de impact van ICT-uitval in de accountancy door weersextremen zoals extreem veel regen, denk aan wateroverlast, daardoor stroomuitval of uitval van ICT geleverd door derden (telefonie, internet, cloud).

Het onderzoek heeft zich specifiek gericht op MKB-accountancybedrijven, deze MKB-accountancybedrijven zijn om verschillende redenen markant;

1. De accountancysector binnen het MKB maakt in grote mate gebruik van ICT.
2. Klanten van accountancybedrijven maken veelal gebruik van applicaties en gegevens die op de ICT-omgeving van MKB-accountancybedrijven staan.
3. MKB-accountancybedrijven moeten voldoen aan door de overheid opgelegde wetgeving.

Het CBS (2014) beschrijft dat het gebruik van ICT-middelen binnen de financiële en dienstverleningssector (midden/groot MKB) erg hoog is. Dit gegeven maakt de accountancy sector interessant voor dit onderzoek. Daarnaast wordt verondersteld dat klanten van MKB-accountancybedrijven veelal gebruik maken van de ICT van deze MKB-accountancybedrijven. Als laatste moeten MKB-accountancybedrijven voldoen aan wettelijke verplichtingen als het gaat over de jaarrekening controle.

Het onderwerp van dit onderzoek is dan ook gericht op het beantwoorden van de vraag:

'In welke mate zijn Nederlandse MKB-accountancybedrijven voorbereid op uitval van ICT door Extreme Weather Events (EWE)?'

Deze onderzoeksvraag is onderverdeeld in drie deelvragen:

1. Hoe groot is de bereidheid tot klimaatadaptatie?
2. Wat is de economische en operationele capaciteit voor adaptatie?
3. Wat is de potentiële impact?

De resultaten dragen bij aan de kennis van ICT en klimaatadaptatie binnen het MKB en draagt kennis bij aan het nationale programma 'Nationale Adaptatie Strategie (NAS)' van de Nederlandse overheid. Daarnaast krijgt de MKB-sector hierdoor inzicht in risico's en de mate van voorbereiding en biedt handelingsperspectief om de risico's op een adequate manier te kunnen behandelen. Expliciet wordt alleen de mate van voorbereiding op uitval van ICT in de accountancy door extreem weer (EWE) onderzocht. De scope van het onderzoek richt zich alleen op Nederland. De risicofactoren van extreem weer en klimaatveranderingen rondom naar buiten Nederland geplaatste ICT, denk aan data bij buitenlandse cloud-dienstproviders, valt buiten de scope van dit onderzoek.

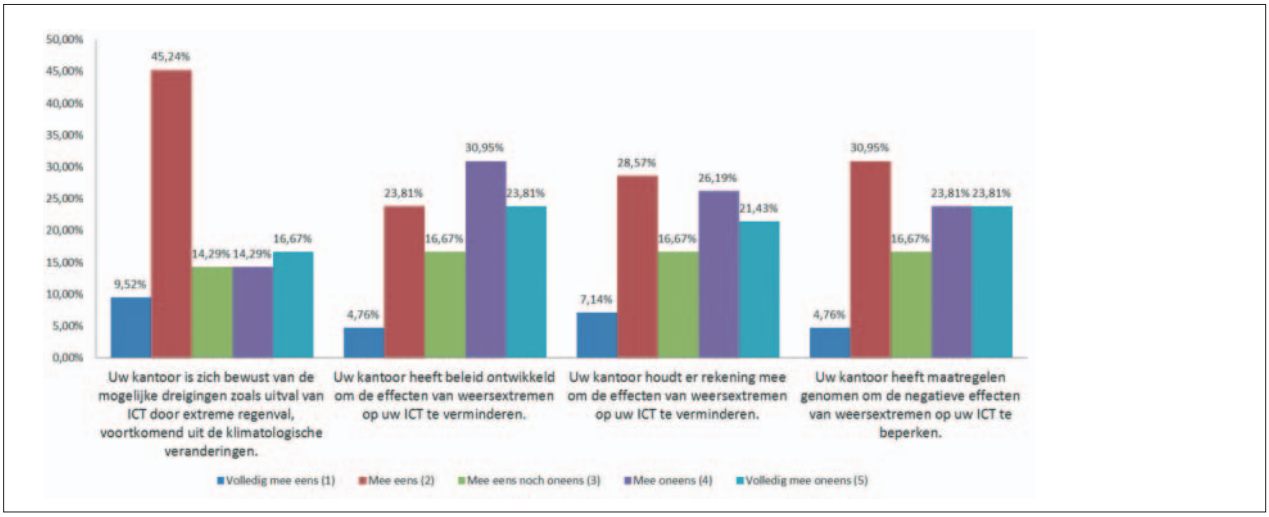
Resultaten

Hoe groot is de bereidheid tot klimaatadaptatie?

Met deze onderzoeksvraag is vastgesteld hoe groot de bereidheid is tot klimaatadaptatie en in welke mate MKB-accountancybedrijven zich bewust zijn van de effecten en de daarmee gepaard gaande dreigingen die klimaatveranderingen in de toekomst mogelijk veroorzaken. Ook is onderzocht In hoeverre MKB-accountancybedrijven rekening houden met klimaatverandering, of er beleid voor is ontwikkeld en/of er maatregelen zijn genomen om discontinuïteit van hun ICT te beperken. De volgende conclusies kunnen uit het onderzoek worden getrokken:

- Meer dan de helft (54,7%) van alle MKB-accountancybedrijven geeft aan zich bewust te zijn van de mogelijke dreigingen voortkomend uit klimatologische veranderingen.
- Meer dan de helft (54,7%) van alle MKB-accountancybedrijven heeft geen beleid ontwikkeld om de effecten van weersextremen met gevolg uitval van ICT te verminderen.
- 30% van alle MKB-accountancybedrijven heeft beleid ontwikkeld om de effecten van weersextremen met gevolg uitval van ICT te verminderen.
- Bijna de helft (47,6%) van alle MKB-accountancybedrijven heeft geen maatregelen getroffen om discontinuïteit van hun ICT door klimaatveranderingen te beperken.
- 35% van alle MKB-accountancybedrijven heeft maatregelen getroffen om discontinuïteit van hun ICT door klimaatveranderingen te beperken.

Jan Frederik Prins is werkzaam als adviseur bij KPN Chief Information Security Officer en Jan is bereikbaar via prinsjf@gmail.com



Grafiek 1

Grafiek 1: Overzicht reacties bereidheid tot klimaatadaptatie.

Kort samengevat kan worden geconcludeerd dat een substantieel deel van de MKB-accountancybedrijven zich bewust is van het veranderende klimaat in Nederland en de implicaties hiervan op de continuïteit van hun bedrijfsvoering. Dit heeft er voor een kleiner deel van deze bedrijven zelf toe geleid om beleid hiervoor te ontwikkelen en maatregelen te treffen om discontinuïteit van hun ICT door klimaatveranderingen te beperken.

Wat is de economische en operationele capaciteit voor adaptatie?

Met deze onderzoeksvraag is vastgesteld in welke mate MKB-accountancybedrijven financiële en operationele middelen hebben om te investeren in maatregelen en/of MKB-accountancybedrijven verwachten dat de overheid verantwoordelijkheid moet nemen door klimaatadaptatie maatregelen te treffen. De volgende conclusies kunnen uit het onderzoek worden getrokken:

- Een meerderheid (64,2%) geeft aan dat zij over voldoende operationele middelen beschikken om adaptatie maatregelen te treffen.
- Een groot deel (69%) van de respondenten geeft aan dat zij over voldoende financiële middelen beschikken om adaptatie maatregelen te treffen.
- Een derde (33,3%) geeft aan dat zij niet verwachten dat de overheid klimaat adaptatie maatregelen moet treffen.
- Nagenoeg een derde (32%) verwachten dat de overheid klimaatadaptatie maatregelen treft.

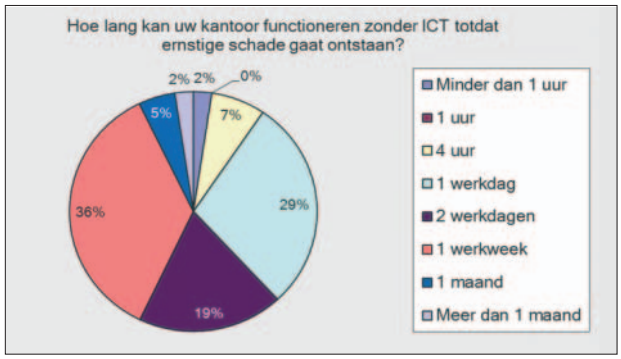
Kort samengevat kan worden vastgesteld dat een flinke meerderheid van de MKB-accountancybedrijven over voldoende financiële en operationele middelen beschikt om maatregelen te treffen en een relatief klein gedeelte van mening is dat dit de verantwoordelijkheid van de overheid is.

Meer dan de helft (54,7%) geeft aan tussen 2 werkdagen en 1 werkweek ernstige schade op te lopen

Wat is de potentiële impact?

Met deze onderzoeksvraag is vastgesteld wat de potentiële impact is voor MKB-accountancybedrijven als een EWE zich manifesteert en hierdoor ICT uitvalt. Er is vastgesteld hoe lang kan een MKB-accountancybedrijf zonder ICT kan zonder beperkte of ernstige schade op te lopen en wat voor maatregelen er zijn getroffen om de impact te verkleinen. De volgende conclusies kunnen uit het onderzoek worden getrokken:

- Meer dan een derde van alle respondenten (38,1%) geeft aan binnen minder dan 1 uur en 1 werkdag ernstige schade op te lopen.
- Meer dan de helft (54,7%) geeft aan tussen 2 werkdagen en 1 werkweek ernstige schade op te lopen.
- Een ruime meerderheid van 85,7% geeft aan dat binnen minder dan 1 uur en 1 werkdag beperkte schade zal ontstaan na uitval van ICT.
- 14,3% geeft na 2 werkdagen tot 1 werkweek beperkte schade op te lopen.



Grafiek 2

Grafiek 2: Cirkeldiagram mate van niet functioneren voordat ernstige schade ontstaat.

Kort samengevat kan worden geconcludeerd dat dat MKB-accountancybedrijven maar zeer beperkt zonder ICT kunnen. 92% van alle MKB-accountancybedrijven kan niet langer dan 1 werkweek zonder ICT zonder ernstige schade op te lopen.

In welke mate zijn afhankelijkheden van ICT in kaart gebracht?

Met deze onderzoeksvraag is vastgesteld in welke mate MKB-accountancybedrijven hun afhankelijkheden van ICT in kaart hebben gebracht en in welke mate MKB-accountancybedrijven zich bewust zijn van hun afhankelijkheid van ICT en in welke mate zijn klanten van afhankelijk van de ICT van MKB-accountancybedrijven. De volgende conclusies kunnen uit het onderzoek worden getrokken:

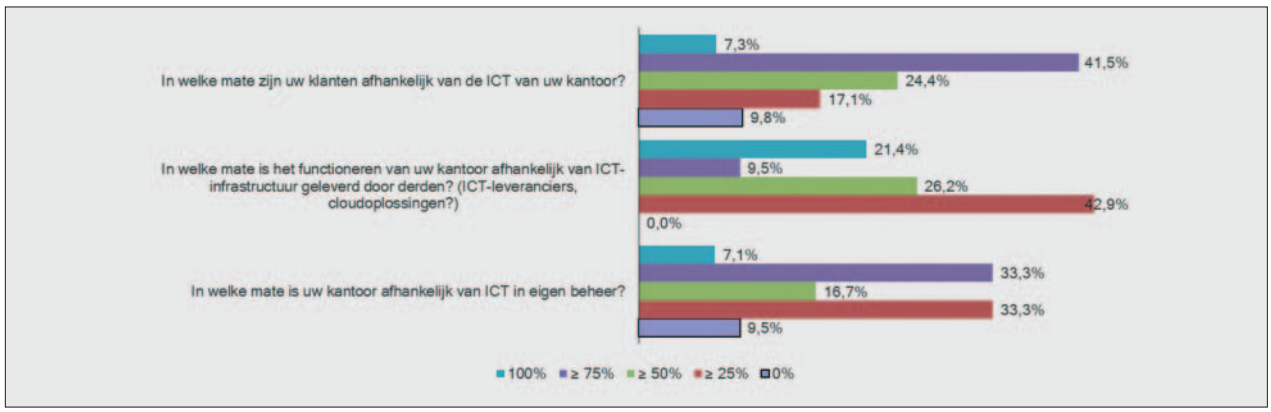
- Een grote meerderheid van 69% heeft hun afhankelijkheid van ICT in kaart gebracht.
- 90% van de MKB-accountancybedrijven geeft aan dat hun klanten voor 25 tot 100% afhankelijk zijn van de ICT die hun MKB-accountancybedrijf host.
- 87% van de MKB-accountancybedrijven geeft aan tussen de 25 en 100% afhankelijk te zijn van ICT geleverd door derden (ICT-leveranciers, cloudoplossingen).
- 92% van de MKB-accountancybedrijven geeft aan tussen de 25 en 100% afhankelijk te zijn van ICT in eigen beheer.

Grafiek 3: Overzicht mate van afhankelijkheid ICT.

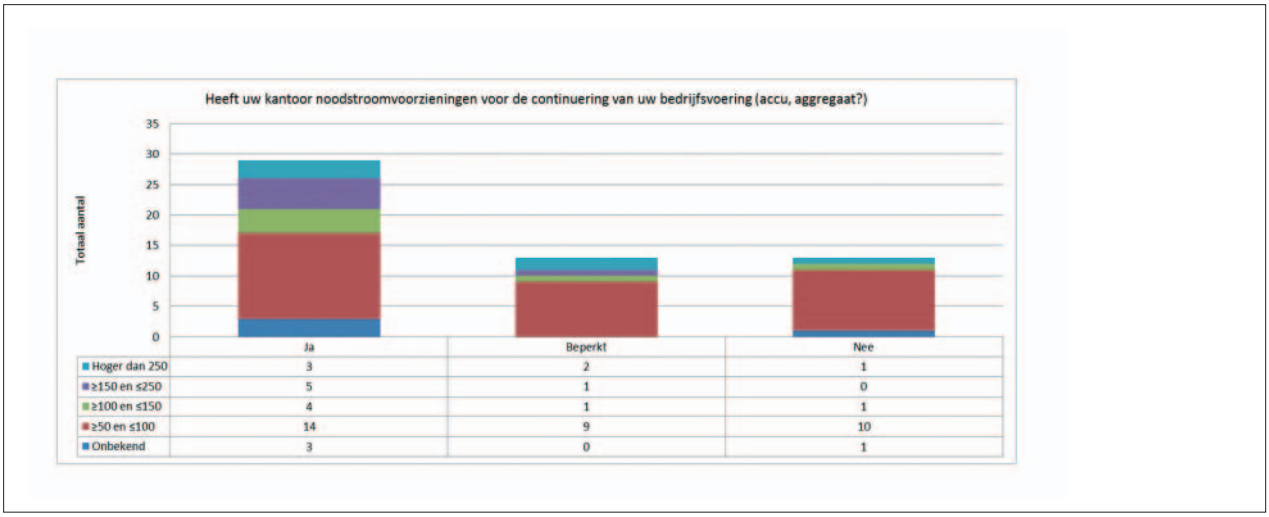
De impact van EWE's op MKB-accountancybedrijven en hun klanten kan dus groot zijn. Een overgrote meerderheid van de MKB-accountancybedrijven heeft de afhankelijkheid van ICT in kaart gebracht, waaruit geconcludeerd kan worden dat deze bedrijven zich bewust zijn van de impact bij uitval. Opmerkelijk is het grote percentage van klanten die in meer of mindere mate gebruik maken van ICT die gehost is bij MKB-accountancybedrijven. Dit betekent dat bij lokale effecten van EWE's bij MKB-accountancybedrijven dit ook impact kan hebben op de bedrijfsvoering van hun klanten. Het uitbesteden van ICT door MKB-accountancybedrijven aan ICT-leveranciers of hostingpartijen kan voordelen opleveren in het geval van lokale effecten van EWE's bij MKB-accountancybedrijven zoals wateroverlast, de ICT is dan veilig gehost op een andere plek en is dus niet beschadigd. Een nadeel hiervan is dat de afhankelijkheid van de vitale infrastructuur zoals internet en dataconnecties hierdoor toeneemt. Bij uitval van bijvoorbeeld een straatkast of wijkcentrale door EWE's is het MKB-accountancybedrijf ook geraakt, ondanks dat zij misschien zelf geen schade heeft opgelopen. De conclusie die hieruit kan worden getrokken is dat ICT bij MKB-accountancybedrijven voor een deel zelf wordt gehost, voor een deel bij externe partijen. Hierbij wordt het risico gespreid en neemt de potentiële impact veroorzaakt door EWE's op lokaal niveau af. Dit is afhankelijk van het scenario of de effecten van EWE's lokaal geconcentreerd zijn of een groter gebied bestrijken.

Impactbeperkende maatregelen

Dit deel van het onderzoek heeft onderzocht in welke mate MKB-accountancybedrijven maatregelen hebben getroffen om eventuele impact van calamiteiten te beperken zoals als gevolg van extreme Weather Events. Het gaat hier over primaire maatregelen zoals noodstroomvoorziening en



Grafiek 3



Grafiek 4

continuiteitsplannen, het inrichten volgens een Business continuity standaard is hierin al weer een stap verder. De volgende conclusies kunnen worden getrokken:

- 69% van de MKB-accountancybedrijven heeft volledig of beperkte noodstroomvoorzieningen ingericht.
- 31% van de MKB-accountancybedrijven is direct geraakt op het moment dat de stroomvoorziening uitvalt.
- 43% van de MKB-accountancybedrijven heeft continuïteits- of recoveryplannen opgesteld.
- Alle 42 MKB-bedrijven (100%) hebben aangegeven dagelijks een backup van hun (klant) gegevens te maken.
- Van alle bevraagde MKB-accountancybedrijven geven 9 bedrijven (21%) aan gebruik te maken van een van een (ISO-)standaard waarmee continuïteit is ingericht, zoals bijvoorbeeld de ISO22301 business continuity standaard.

Grafiek 4: Overzicht noodstroomvoorziening.

Opvallend is het hoge percentage MKB-accountancybedrijven dat aangeeft volledige of beperkte noodstroomvoorzieningen te hebben ingericht. Hiermee wordt de afhankelijkheid van stroom geleverd door de netbeheerders iets beperkter. Stroomuitval van korte duur (vermoedelijk enkele uren) kunnen door deze noodstroomvoorzieningen worden opgevangen. Iets minder dan de helft van de MKB-accountancybedrijven heeft continuïteits- of recoveryplannen opgesteld om tijdens een calamiteit hun primaire bedrijfsvoering op een alternatieve wijze te kunnen continueren en alle MKB-bedrijven geven aan dagelijks een backup van hun data te maken. Hierdoor neemt de kwetsbaarheid van MKB-bedrijven in redelijke mate af. In veel gevallen zal na een calamiteit de data nog beschikbaar zijn en is er nagedacht over alternatieve werkwijzen om de primaire bedrijfsvoering voort te zetten en hiermee de schade te beperken. Opvallend is dat een vijfde van de MKB-accountancybedrijven gebruikt maakt van een (ISO) standaard om de continuïteit actief te beheren door het inventariseren van kritieke bedrijfsprocessen, risico's en het treffen van maatregelen. Hierdoor zal de kwetsbaarheid van MKB-accountancybedrijven verder afnemen en zijn deze bedrijven meer in control.

Conclusies

Samenvattend is te stellen dat MKB-accountancybedrijven in beperkte mate zijn voorbereid op uitval van ICT veroorzaakt door de effecten van EWE's. De impact op de bedrijfsvoering door uitval van ICT is groot. De effecten van EWE's zoals stroomuitval, het verliezen van data of telefoonverbindingen zijn vaak generieke risico's die ook door andere dreigingen veroorzaakt kunnen worden. Genomen maatregelen zoals noodstroomvoorzieningen en het opstellen van continuïteitsplannen zorgen voor een geringere impact. Een flinke meerderheid geeft aan over voldoende financiële en operationele middelen te beschikken om maatregelen te treffen maar een minderheid heeft deze ook daadwerkelijk getroffen.

Aanbevelingen

Op basis een literatuurstudie en de analyse van de verzamelde data verkregen uit MKB-accountancybedrijven doen wij kort samengevat de volgende aanbevelingen:

1. **Bepaal de kritieke processen en assets**
   Hoewel een meerderheid van de MKB-accountancybedrijven aangeeft hun afhankelijkheid van ICT in kaart te hebben gebracht is het ook van groot belang om vast te stellen welke bedrijfsprocessen het meest belangrijk (kritiek) zijn en wat de maximale uitvalsduur van deze processen is voordat ernstige schade gaat ontstaan. Dit kan bijvoorbeeld door het uitvoeren van een Business Impact Analyse (BIA). Stel vast hoe deze kritieke processen

samenhangen en inventariseer hoe de keten is opgebouwd. Welke middelen, mensen gebouwen en leveranciers zijn nodig om het proces uit te voeren. Denk hierbij aan bijvoorbeeld specifieke hard- of software of externe infrastructuur.

2. **Inventariseer risico's**
   Nadat de kritieke processen en assets zijn vastgesteld is het raadzaam om te inventariseren welke risico's een bedreiging vormen voor deze processen of assets. Het risico profiel wordt vastgesteld door het bepalen van de kans van optreden en de impact. Denk hierbij aan externe en interne risico's. Externe risico's zijn in de context van dit onderzoek de effecten van EWE's zoals wateroverlast, overstroming, uitval elektriciteit of dataverbindingen.
3. **Selecteer maatregelen**
   Na het vaststellen van de relevante risico's die de kritieke processen of assets kunnen bedreigen is het verstandig om overwogen maatregelen te treffen. Dit betekent dat de investering om een maatregel te treffen in verhouding moet staan met de eventueel verwachte schade. Voorbeelden van maatregelen binnen het kader van het onderzoek zijn het op voorhand verzorgen van een vaste en mobiele dataverbinding, noodstroomvoorzieningen, continuïteitsplannen om processen op een alternatieve wijze uit te voeren.
4. **Evalueer**
   Analyseer periodiek welke bedrijfsprocessen of assets van kritiek belang zijn, door veranderende omstandigheden kan het zijn dat processen meer kritisch of minder kritisch zijn geworden. Dit geldt ook voor de risico-inventarisatie, het periodiek inventariseren van risico's zorgt ervoor dat deze op een juiste waarde worden ingeschat. Op basis van de nieuwe inzichten kunnen eventuele maatregelen om het risico te verkleinen of weg te nemen worden aangepast.

Referenties

CBS (2014). ICT kennis en economie 2014.

Centre for Economic and Business Research (2014). European economic impact study Sage Enterprise Market Europe.

Füssel, H., & Klein, R. J. (2006). Climate change vulnerability assessments: An evolution of conceptual thinking. Climatic Change, 75(3), 301-329.
KNMI (2014). KNMI klimaat scenario's 2014. Retrieved 03/10, 2015, from http://www.klimaatscenarios.nl/

Lenderink, G., van den Hurk, B., Tank, A. K., van Oldenborgh, G., de Vries, E van Meijgaard KNMI H, & Beersma, J. (2014). Publications, presentations and other activities preparing local climate change scenarios for the netherlands using resampling of climate model output. 2014. Environmental Research Letters, 9(11), 115008.

Luiijf, E. A., Burger, H. H., & Klaver, M. H. (2003). Critical (information) infrastructure protection in the netherlands. Paper presented at the GI Jahrestagung (Schwerpunkt" Sicherheit-Schutz Und Zuverlässigkeit"), pp. 9-19.

Ministeries van VROM, V&W, LNV, EZ IPO, VNG, Unie van Waterschappen (2007). Maak ruimte voor klimaat! nationale adaptatiestrategie - de beleidsnotitie

NBA (2015). Nadere voorschriften controle- en overige standaarden (NV COS). Retrieved 18/05, 2015, from https://www.nba.nl/wet-en-regelgeving/beroepsregels/hra/

PBL, K. (2014). Klimaatverandering, samenvatting van het vijfde IPCC-assessment en een vertaling naar nederland.

Runhaar, H., Gilissen, H. K., Uittenbroek, C., Mees, H., & van Rijswick, M. (2014). Publieke en private verantwoordelijkheden voor klimaatadaptatie: Een juridisch-bestuurlijke analyse en eerste beoordeling.

SRA (2014). Praktijkhandleiding 'IT in de jaarrekeningcontrole SRA Vaktechniek.

Rence Damming

MELDPLICHT DATALEKKEN

Het implementatieverhaal vanuit de praktijk van KPN

Op 5 juni 2012 werd na geruime tijd en discussie over de implementatie van de Europese richtlijn 2009/136/EC de meldplicht datalekken in Nederland verankerd in de Telecommunicatiewet. In aanloop op deze wetsimplementatie werd er vanuit KPN, naast de lobby over vorming van deze wet, geanticipeerd op de wijze waarop dit in de bestaande processen van KPN moest gaan passen. In dit artikel wil ik jullie graag meenemen in de uitdagingen, do's en don'ts en best practices (learning by doing).

Eerder gepubliceerd op het Kennisplatform van Cqure op 1 oktober 2015

Wettelijk kader

In de Telecommunicatiewet is de meldplicht datalekken verankerd in artikel 11.3a. Deze meldplicht geldt voor het geval er, ondanks de genomen veiligheidsmaatregelen op grond van artikel 11.3 Tw, toch sprake is van inbreuken op de beveiliging die nadelige gevolgen (kunnen) hebben voor de veiligheid van de persoonsgegevens. Aanbieders zijn verplicht dergelijke inbreuken onverwijld te melden bij de ACM (Autoriteit Consument en Markt). De ACM kan vervolgens nagaan of de inbreuk gevolgen kan hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft, of de door de aanbieder genomen maatregelen als afdoende kunnen worden beschouwd, en of er aanleiding is de abonnee wiens gegevens het betreft te informeren over de inbreuk. Indien de beveiligingsinbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de gebruikers en/of abonnees, moeten ook zij op grond van artikel 11.3a Tw worden ingelicht.

De toezichthouder

Bij de implementatie van de meldplicht datalekken in de Telecommunicatiewet (Tw) werd de voormalige OPTA, sinds 2013 verder onder de naam ACM, aangewezen als toezichthouder op het artikel 11.3a Tw. De ACM is niet het directe meldpunt maar behandelt wel inhoudelijk de gemelde datalekken. Voor de toezichthouder is het met name van belang dat gemelde datalekken volledig, tijdig en correct worden afgewikkeld. De rol van de toezichthouder is dan ook dusdanig beperkt dat de toezichthouder overziet of de verantwoordelijke telecommunicatieaanbieder zich houdt aan de verplichtingen zoals beschreven in de wet en zonodig bijstuurt.

Meldpunt datalekken

De toezichthouder op de meldplicht datalekken in de Tw is niet het meldpunt waar datalekken gemeld dienen te worden. Deze rol is weggelegd voor het Agentschap Telecom (AT), onderdeel van het Ministerie van Economische Zaken. AT zorgt ervoor dat de meldingen kunnen worden geregistreerd en worden doorgegeven aan de toezichthoudende instantie. Het AT onderhoudt dan ook een nauwe samenwerking met ACM als het gaat om de meldplicht datalekken. Om een datalek te kunnen melden, kan de openbare telecommunicatieaanbieder, hierna Telco, gebruik maken van een elektronisch registratieformulier of telefonisch via een 24/7 bemande registratiedesk.

Impact en risico's

Zoals beschreven in het wettelijk kader, dienen alle vastgestelde datalekken onverwijld te worden gemeld aan de betrokkene en aan de toezichthouder. ACM stelt zich op het standpunt dat 'onverwijld' betekent 'binnen 24 uur'. Om een melding volledig te maken, dient dan allereerst te worden vastgesteld wat de impact op de persoonlijke levenssfeer is voor de betrokkene en hoe het lek, indien mogelijk, zo snel mogelijk gedicht kan worden. Dit vereist de nodige inrichting in je organisatie, hierover leest u later meer. Indien de betrokkene niet onverwijld een melding ontvangt, resulteert dit in twee mogelijke consequenties voor de Telco:

1. Een boete of last onder dwangsom vanuit de toezichthouder voor het niet naleven van de Tw
2. De mogelijkheid dat een betrokkene naar de media stapt en de betreffende Telco alsnog geconfronteerd wordt met het datalek via de media, hetgeen mogelijk ook weer leidt tot punt 1 met alle nodige publiciteitsschade

Het niet melden van een datalek waarbij de persoonlijke levenssfeer van de betrokkene geschaad is, zou zelfs zonder meldplicht datalekken, onverstandig zijn. Het kan immers zorgen voor een boomerang effect, wat natuurlijk alleen maar versterkt wordt wanneer daar ook nog een wettelijk voorschrift voor ligt. Het is daarom evident dat er een snelwerkend proces wordt geïmplementeerd dat zorgt voor een juiste opschaling en communicatiestructuur in de organisatie. Dit resulteert in strakke richtlijnen en protocollen over hoe om te gaan met datalekken. Doordat vooraf niet alle mogelijke incidenten zijn te scharen onder het datalekkenprotocol, is het protocol vrijwel altijd aan verandering en verbetering onderhevig.

Inventariseren organisatiestructuur

Maar hoe implementeer je nu een dergelijk proces of protocol in je organisatie? Ik denk dat dit verschilt per type organisatie, de grote ervan, de hoeveelheid klantgegevens die een bedrijf verwerkt, de complexiteit van de processen en systemen die voor de verwerking van gegevens zorgen en de wijze waarop organisaties gegevens verzamelen. Het is ongetwijfeld zo dat een bedrijf van een kleinere omvang sneller in staat is om kortere lijnen te hebben tussen systeembeheerders, communicatie-experts en verzamelaars van persoonsgegevens. Bij grotere bedrijven ligt dit vaak complexer. Bij een bedrijf als KPN was dit een hele uitdaging. KPN bestaat uit ruim 31000 medewerkers, verwerkt dagelijks miljoenen persoonsgegevens van haar klanten, heeft een bijzonder complexe technische infrastructuur en honderden, misschien wel duizenden verschillende klantingangen. Denk daarbij aan retailers, winkels, online en dat weer onderverdeeld in verschillende merken. Omdat KPN ook voor de invoering van de meldplicht datalekken wel eens met het fenomeen datalekken in aanraking kwam, was dit niet geheel nieuw waar het ging om de technische oplossingen en mitigerende acties. Maar het feit dat bepaalde meldingen via een nieuw communicatieproces binnen striktere tijdslijnen moesten worden opgelost, was wel een nieuwe invalshoek.

Security vs Privacy bij datalekken

Binnen KPN was er voor 2011 sprake van een intern meldingsprotocol voor de zogeheten 'security incidenten'. Hieronder vielen destijds ook al de privacyincidenten zoals datalekken, maar deze werden niet als zodanig geclassificeerd en werden bovendien in veel gevallen naar goeddunken van de behandelende Security

Officer individueel opgelost en gecommuniceerd. Het leek daarom ook een logische stap voor KPN om het bestaande securityincidentproces als uitgangspunt te hanteren voor het inrichten van een centraal datalekkenproces in het kader van de meldplicht. Een groot voordeel bij het bestaande securityincidentproces was dat er reeds een bedrijfsbrede ingang bestond waar datalekken gemeld konden worden. Ook werden medewerkers van KPN door het bestaan van het securityincidentproces reeds aangespoord om verlies/vermissing van bedrijfsgoederen en eventuele misstanden en vermoedens van lekken aan de zogeheten Helpdesk Security door te geven. Een ander groot voordeel bij het aanpassen van het huidige securityincidentproces, was dat het eerste wat je bij een datalek probeert te bereiken, het daadwerkelijk dichten van het lek is. Natuurlijk is dat niet in alle gevallen mogelijk, een incident kan natuurlijk ook voorkomen door een verkeerde administratieve eenmalige handeling of het feit dat een postsorteermachine een eenmalige storing heeft, waardoor facturen met daarin persoonsgegevens in de verkeerde enveloppe met een andere bestemming belanden. Het uitgangspunt om een stringent securityincidentproces te hanteren om zo snel mogelijk tot de kern van het probleem te komen, was voor KPN een logische keuze.

Spreken met business owners en stakeholders

Het inrichten van een datalekkenproces in een grote complexe organisatie vereist een aantal noodzakelijke handelingen. Allereerst moeten alle betrokken en verantwoordelijke collega's bekend worden gemaakt met de noodzaak om datalekken te melden en de voorziene oplossing binnen KPN. Hiervoor zijn wij simpelweg met alle interne betrokken afdelingsmanagers gaan praten, hebben de noodzaak geïllustreerd in een 'levendige' presentatie en over de oplossing gebrainstormd. Pas toen alle verantwoordelijke afdelingen en collega's akkoord waren met het voorstel, zijn wij overgegaan tot implementatie. Het proces dat vandaag de dag binnen KPN wordt gehanteerd, wordt daarom ook door alle betrokkenen gedragen. Bijgaande opsomming geeft een idee welke afdelingen bij dit proces betrokken zouden moeten worden:

- Klantcontact afdelingen
- Communicatie
- Juridische zaken en regelgeving
- Security
- Information Security, Compliance en Risk specialisten
- Public Affairs
- IT-afdelingen
- Vele anderen

Integreren of separaat proces?

Tijdens de ontwikkeling van het datalekkenproces zijn er momenten geweest waarin er werd overgewogen om het datalekkenproces los van de bestaande processen op te zetten. Een groot voordeel daarbij is dat dit geheel een eigen inrichting zou krijgen, waardoor meer flexibiliteit, minder noodzaak voor verandering teweeg brengt in bestaande registratiesystemen en organisatie en mogelijk sneller ingezet kan worden dan bij een aanpassing van de bestaande procesgang. Juist omdat het verzamelen van de meldingen een dusdanig grote rol betekende in de afwikkeling van de datalekken werd er door KPN uiteindelijk toch gekozen voor een integratie met bestaande processen en verscherping van de interne communicatie-uitingen en de protocollen voor het extern benaderen van klanten over datalekken.

Aanpassen proces

Bij het aanpassen van het proces, was het vooral van belang dat er bij elk datalek na binnenkomst van een melding bij de Security Helpdesk een select team van mensen werd ingeschakeld. Dit noemen wij intern: het Incident Response Team. Het Incident Response Team wordt geleid door een Security Manager, vaak in het bedrijfssegment waar het incident zich heeft voorgedaan, of waar het incident als eerste is genotificeerd. De Security Manager vormt een team met daarin in ieder geval een compliance manager, een communicatiespecialist en, in geval van een technisch incident, een technisch expert die de technische oplossing verzorgt. Naast de algemene leiding door de Security Manager verzorgt de compliance manager de communicatie naar de toezichthouder, waarborgt de communicatiespecialist dat de interne alsmede de externe communicatie zorgvuldig verloopt en zorgt de IT specialist waar nodig er voor dat het technisch euvel wordt verholpen.

Bewustwording en communicatie

Zoals al eerder genoemd in de afweging om het datalekkenproces al dan niet te integreren in de bestaande processen, is het evident dat meldingen van potentiële datalekken intern, bij voorkeur centraal, worden geregistreerd. Dit om een overzicht te bewaken en om er voor te zorgen dat de juiste mensen gaan rennen. In het geval van KPN was dit middels het securityincidentproces al centraal opgehangen, maar diende het bewustzijn onder alle medewerkers ten aanzien van het bestaan van de meldplicht datalekken alsook de noodzaak om ook twijfelgevallen te melden bij de centrale Security Helpdesk, wel vergroot te worden. Om dit te realiseren heeft KPN een mix van communicatiemiddelen opgetuigd om zodoende alle medewerkers te bereiken. Hierbij kan gedacht worden aan berichten op het Intranet, promotionele posters, een interne awareness-film, verplichte cursussen, workshops en presentaties door de hele organisatie heen op zeepkisten en managementbijeenkomsten. Hoewel de eigenlijke insteek was om zoveel mogelijk van de bewustwordingspresentatie als een cascade langs de lijnen van het management neer te laten dalen bij alle medewerkers, werd dat in de praktijk toch vaak het doorsturen van de presentatie per e-mail. Gelukkig leidde dit vervolgens tot vragen aan de Privacy Officer om het verhaal nader toe te lichten. Na een grootschalige communicatiecampagne, zou iedere medewerker een potentieel datalek moeten kunnen herkennen en melden bij de interne Security Helpdesk. Het werd nu tijd om het proces te testen.

Pilot over werking proces

Al voor de inwerkingtreding van meldplicht datalekken op 5 juni 2012 had KPN ruim de gelegenheid om het proces intern te testen. Spoedig bleek dat de verzameling van meldingen zich ophoopte en dat er een noodzaak voor het categoriseren van verschillende typen potentiële datalekken ontstond. Ondanks het feit dat er verscheidene meldingen binnenkwamen op de centrale helpdesk die helemaal geen datalek bleken te zijn, was het toch goed dat ook deze meldingen serieus naar de melder werden teruggekoppeld, waarbij een en ander nog eens werd uitgelegd om zodoende ook het melden te blijven stimuleren. Mijn motto en boodschap naar de organisatie was in die periode (en nog steeds) dan ook: "Als je twijfelt, gewoon melden. Ik heb liever 100 meldingen teveel dan 1 te weinig". Dit motto bleek goed te werken. Vervolgens was het de taak aan het Incident Response Team om de meldingen te analyseren en te behandelen. Gaandeweg leerde wij dan ook dat bepaalde meldingen konden worden afgehandeld door de centrale Security Helpdesk en andere meldingen een diepgaander onderzoek vereisten. Snel werd duidelijk dat een onderlinge afstemming met zowel de melder (intern en extern) als de interne specialisten onontbeerlijk was. Na wat vallen en opstaan, wat met name op het gebied van verantwoordelijkheid lag, konden we gezamenlijk met alle stakeholders vaststellen dat het datalekken proces, geïntegreerd in de bestaande Security procesgang, werkt.

De eerste melding

Op 5 juni 2012 trad de meldplicht datalekken in werking. Feitelijk bleek er weinig te veranderen, daar KPN reeds over en weer contact had met de toezichthouder, ook met het oog op de komende meldplicht. Belangrijke les bij deze onderlinge werkwijze was: bij twijfel bellen en verwachtingen uitwisselen. Dankzij een goede samenwerking met de ACM werd het KPN vrij snel duidelijk wat er verwacht werd aan de zijde van de toezichthouder en bleek het nuttig om periodiek evaluatiegesprekken te voeren.

Complicaties bij interpretatie meldplicht

Natuurlijk bestaan er veel onduidelijkheden over de meldplicht datalekken en met name over de interpretatie van het datalek an sich. Ook bestond er vooral in de beginfase onduidelijkheid over welke zaken gemeld diende te worden en welke zaken niet. Wanneer leidt een incident of datalek tot een schending van de persoonlijke levenssfeer? Wanneer classificeer je een gegeven als een persoonsgegeven? Om daar maar heel kort over te zijn: dit zal je per geval moeten gaan beoordelen. Het is namelijk geen gegeven dat het lekken van bepaalde data direct of indirect tot een schending van de persoonlijke levenssfeer zal gaan leiden, noch is het generiek te bepalen of een gegeven in combinatie met andere gegevens weer te herleiden is tot een natuurlijk persoon. Al deze zaken zal je case-by-case moeten beoordelen en telkens opnieuw moeten afwegen. Een ander discussieonderwerp waar wij intern tegen aanliepen is de vraag of ook gegevens van zakelijke gebruikers onder de meldplicht vallen. Daaruit hebben wij geconcludeerd dat zolang dit tevens eindgebruiker gegevens betreffen en in de essentie de persoonlijke levenssfeer van deze eindgebruiker geschaad is, dit als datalek als bedoeld in de Tw classificeert en dus onder de meldplicht valt. In het geval KPN als een bewerker van gegevens optreedt, dient een eventuele melding onverwijld aan de betreffende verantwoordelijke te worden gedaan, zodat deze op zijn beurt aan de meldplicht kan voldoen.

Afstemmen met de toezichthouder

Na de interne implementatie bleek al vrij snel de wens te bestaan om duidelijk de verwachtingen van de toezichthouder scherp te krijgen. Zoals al eerder genoemd heeft KPN dit in goed overleg met de toezichthouder kunnen evalueren. Belangrijk om in het achterhoofd te houden is dat de verantwoordelijkheid van de juiste en tijdige afwikkeling, communicatie en oplossing geheel bij de verantwoordelijke berust. In de meeste gevallen is dit simpelweg het gebruiken van je common sense, oftewel je boerenverstand. Ik daag vaak mijn eigen collega's uit door de vraag te stellen: "Hoe zou je het zelf vinden, als jouw gegevens worden gelekt?" Dit leidt altijd tot de nodige discussie, waarna vaak de juiste besluiten volgen.

Learning by doing

Zoals ik aan het begin van het artikel noemde, is het implementeren van de meldplicht datalekken, een kwestie van learning by doing. Niet in de laatste plaats omdat je niet te lang in de 'theoretische discussie' wilt blijven hangen. Het is goed om je aanpak te overdenken, maar wacht niet te lang met de executie. Toen ik vroeger bordspellen met vrienden moest leren op een regenachtige zondag, lazen we ook niet eerst uitvoerig de handleiding of spelinstructies door, maar gingen we na kennisname van de basisuitgangspunten gewoon spelen, wetende dat men gaandeweg het spel vrij snel door krijgt. Ik geloof dat dit bij dit soort verandertrajecten ook het geval is. Ik heb dan ook ten tijde van de implementatie regelmatig geroepen: "We gaan het gewoon doen en we zien wel waar we tegenaan lopen."

Lessen en conclusies

Belangrijk om mee te nemen is denk ik dat je zorgvuldig je plan op stelt, met de juiste stakeholders praat, deze met je mee krijgt, begrijpt dat de communicatie of the essence is, zo veel mogelijk probeert op te lijnen met reeds bestaande initiatieven binnen jouw organisatie, waar mogelijk afstemt met de toezichthouder en uiteindelijk beseft dat het implementeren van een dergelijk traject een levendige en veranderlijke exercitie is. Ik kan nu na ruim drie jaar dit proces in werking te hebben gezien ook wel te zeggen dat we er als KPN veel van hebben geleerd en we zelfs vandaag de dag het proces nog aan het verbeteren zijn, maar dat het proces er staat.

Rence Damming is privacy officer KPN, dit artikel is tot stand gekomen in samenwerking met Jeroen Terstegge.

HOE 'BIG DATA EN MACHINE LEARNING' SMARTPHONES EN TABLETS BESCHERMEN TEGEN MOBILE ATTACKS

Mobiele apparaten verdringen steeds vaker de PC/laptop. Er wordt verbinding gemaakt met vele netwerken, terwijl er op grote schaal een schat aan informatie en software wordt gedownload middels mobile apps. Het risico voor aanvallen en het lekken van data via smartphones is vele malen groter dan ooit. De stortvloed aan mobiele data biedt echter ook enorme kansen. Het is dan wel belangrijk dat kritische beveiligings signalen niet over het hoofd worden gezien.

Wat is er mis met de manier waarop we onze systemen momenteel beschermen?

De traditionele detectie systemen op basis van handtekeningen (signatures) -reeds sinds de jaren 90 populair- zijn niet langer verfijnd genoeg om zelfstandig een voldoende bescherming te bieden. Makers van malware weten al lang dat het volstaat om een piepklein onderdeel van de code van hun malware te veranderen om anti-virus systemen op basis van signatures om de tuin te leiden.

Een beveiligingsoplossing op basis van gedrag (behavioral) is beter, maar ook dat volstaat niet meer. Het is alsof je code in een geïsoleerde omgeving plaatst en die code port met stokken om te zien wat er gebeurt. Is de code veilig als er niets gebeurt? Zeker niet! Makers van malware innoveren en hebben manieren ontwikkeld om het schadelijke gedrag van apps te masceren zolang deze zich in de virtuele detectie systemen bevinden. Denk aan de Volkswagen CO2 test: zodra de systemen door hadden dat de auto op de testbank stond werd de CO2 meting voor de gek gehouden.

Slechts vertrouwen op een Mobile Device Management (MDM/EMM) oplossing (met of zonder "container" die de zakelijke en persoonlijke data scheidt) is eveneens onvoldoende, aangezien deze slechts een zeer beperkt aantal aanvals vectoren in ogenschouw kan nemen.

Om bedreigingen te kunnen voorspellen, moet je inzicht hebben in alle wereldwijd beschikbare mobiele code

Vandaag de dag zijn we getuige van een transformatie van hoe we het meest effectief naar informatie kunnen kijken: met name middels predictive analytics op basis van big data.

Door gebruik te maken van kunstmatige intelligentie en big data is er inzicht in de stijl van coderen die een aanvaller gebruikt. Net zoals kunstenaars kan een aanvaller een eigen manier hebben om dingen te realiseren, of net zoals een schilder een eigen stijl heeft.

Wanneer een aanvaller malware schrijft kan hij vrij eenvoudig de traditionele beveiligingsmethodes om te tuin leiden, maar de predictive analysis techniek zal overeenkomsten ontdekken die de alarmbel doen rinkelen: "He, dit lijkt erg op schadelijke code die we al kennen, dus let op!" Zonder deze big data (en zonder de kunstmatige intelligentie die de betreffende data real time kan verwerken) zal een beveiligingsoplossing niet goed in staat zijn pro-actief, of na het bekend worden van een zero day kunnen voorspellen of een app kwaadaardig is.

Wat nu?

Uit een recente studie blijkt dat 68% van de internationale organisaties in de laatste 12 maanden is geconfronteerd met mobiele aanvallen. Bedrijfsnetwerken moeten uitkijken voor bedreigingen zoals Wirelurker, XAgent, XcodeGhost, Stagefreight en vele anderen. Reactieve beveiligings oplossingen werken niet, terwijl er steeds meer mobiele bedreigingen op ons af komen. Daarom moeten we nadenken over beveiliging, zowel op macro- als op microniveau. Door de omvang van het gebruik van mobiele systemen moet de beveiliging hiervan op een geheel andere manier benaderd worden in deze wereld waarin iedereen en alles met elkaar verbonden is.

We moeten vooruitkijken en anticiperen. De combinatie van big data met kunstmatige intelligentie is een "must" om mobiele bedreigingen te detecteren nog voordat ze schade aanrichten.

Lookout

Jeroen Wijdogen, Senior Engineer Mobile Security @ Lookout, jeroen.wijdogen@lookout.com, 06-12156492

HET IS AAN ONS

Geïnspireerd heb ik dit jaar meerdere malen naar Jaya Baloo (CISO KPN) geluisterd. Haar verhaal over crypto-wars sluit ze immer af met een oproep aan "de community" om de boer op te gaan en te vertellen over onze wereld, de gevaren die wij zien en uit te leggen wat er gebeurt en te gebeuren staat als wetgevers en veiligheidsdenken de overhand zullen krijgen. De privacy,- en securitygemeenschap moeten meer naar buiten treden, uitleggen en duiden. "De man/vrouw op straat" weet niet wat er allemaal speelt, laat staan dat deze begrijpt wat de gevolgen zijn. Het is aan ons om te helpen.

Het is aan ons om kinderen te beschermen. Herinnert u zich de nieuwe Barbie van Mattel nog? Barbie wordt uitgerust met Wifi, neemt alle gesprekken met het kind op en brengt daarmee potentieel de privacy van die kinderen in gevaar. Ik riep onze helpende hackerscommunity op om haar beveiliging te doorbreken om zo aan te tonen dat het beter moet en beter kan. Halverwege november was het dan eindelijk zo ver, Marie-Jo de Leeuw (medeoprichter van Women in Cyber Security) hackte Barbie voor een live publiek tijdens het WTC International City Podium. Het begin van hopelijk een meer privacyvriendelijkere en veiligere Barbie.

Het is aan ons om patiënten te beschermen. Weet u nog waarvoor dokter Chantal van het Zandt strijdt? Zij zamelt geld in om een kort geding te kunnen starten tegen plannen van Minister Schippers. De materiële controles van zorgverzekeraars op mogelijk frauduleuze zorgdeclaraties vormen volgens de dokter een ongeoorloofde inbreuk op de privacy van patiënten en doorbreken het medisch beroepsgeheim. Tijdens controles kunnen de zorgverzekeraars volledige inzage in de dossiers eisen. Schippers lijkt niet gevoelig voor de privacyargumenten, ze stelde dat zorgverzekeraars gewoon toegang moeten hebben tot de dossiers en dat toestemming van patiënten niet nodig is omdat dat een te grote administratieve last zou opleveren. De dokter heeft helaas (nog?) niet het benodigde bedrag bij elkaar kunnen krijgen, echter haar strijd is niet gestreden. Ze heeft bijval in de Tweede Kamer waar Kamerleden Dijkstra en Bergkamp (D66) deze kwestie op de agenda hebben gekregen.

Het is aan ons om gebruikers van social media te beschermen. Ongetwijfeld heeft u van Max Schrems gehoord. Toen hij in 2011 zich begon te verweren tegen Facebook wegens privacyschending, was er vrij weinig aandacht voor zijn zaak. Hij vond zelfs bij het Data Protection Agency geen gehoor. Zijn "PRISM"-klacht bleek wel degelijk grond te hebben, zo bleek uit de uitspraak van het HvJ EU op 6 oktober dit jaar waarmee een einde kwam aan Safe Harbour. Maar dat betekent voor Schrems niet het einde van de strijd: de "class-action suit" tegen Facebook waarin duizenden Facebook-gebruikers stellen dat de privacyvoorwaarden van de sociale netwerksite in strijd zijn met Europees recht, loopt nog steeds.

Er zijn gelukkig altijd mensen die de strijd aan durven en kunnen gaan. Deze mensen moeten wij koesteren. We kunnen de strijd misschien niet altijd zelf aangaan, misschien moet dat ook niet onze rol zijn. Wat wij wel moeten, is zij die de strijd aangaan helpen.

Het is aan ons.

Mr. Rachel Marbus
@rachelmarbus op Twitter

VERSLAG

CAPTURE THE FLAG COMPETITIE

Dinsdag 6 oktober 18.00 uur. Voor de beheerders van de Nederlandse Responsible Disclosure mailboxen zal deze avond als zeer rustig de boeken in zijn gegaan. Ze konden even rustig adem halen, terwijl hackers zich opmaakten voor de jaarlijkse Capture The Flag competitie van het PViB.
Met ruim 100 man sterk reisden ze dit jaar af naar Driebergen om alweer de zesde editie van dit event tot een succes te maken. De uitdaging was dit jaar groter dan ooit. De tanden konden worden stukgebeten op tientallen vragen, samengesteld door beveiligingsexperts van verschillende Nederlandse beveiligingsbedrijven. Mark de Groot, die samen met het KPN RED Team erg succesvol is in wereldwijd georganiseerde Capture The Flag competities, faciliteerde het platform en had een basisset met vragen.
De uitdagingen voor de deelnemers varieerden sterk. Afhankelijk van de moeilijkheidsgraad van de vraag kon er tussen de 50 en 1000 punten per vraag worden verdiend. Naast het feit dat vragen serieuze webapplicatie, cryptografische en forensische capaciteiten vereisten, zorgde ook de soms cryptische vraagstelling voor een extra moeilijkheidsgraad. Oplossingen lagen zeker niet altijd voor de hand en binnen een vraag konden meerdere kwetsbaarheden aanwezig zijn, waarvan er slechts 1 tot de felbegeerde "flaggencode" leidde.
Een van de moeilijkste vragen bleek de multi-level cryptopuzzel te zijn. Deze puzzel bestaat uit meerdere stappen die allemaal goed opgelost moeten worden. Maar met 1 foutje ben je weer terug bij af en begint de puzzel (enigszins aangepast) weer van voren af aan. Een reden om deze in 1 keer goed op te lossen dus! Ook waren er vragen gemaakt waarbij deelnemers SMS-berichten uit opgevangen mobiel radioverkeer moesten zien te vissen of gevraagd werden om malware te identificeren in netwerk packetdumps. Iets nostalgischer waren de vragen waarbij aanwijzingen verstopt zaten in berichten die middels morse of ROT 13 gecodeerd waren. Natuurlijk werden ook de SQL injection, Cross Site Scripting en brute force skills van de deelnemers niet vergeten.

Het team van Fontys nam al snel de leiding en had na 2 uur 28% van de vragen beantwoord. Ze bleken niet meer in te halen en gingen er met de bokaal vandoor.

Maarten Hartsuijker is beveiligingsconsultant en ethisch hacker bij Classity en bereikbaar via pvib@classity.nl

CYBER SECURED

We live in 'smart world' with the deployment of cyber technology all around us, and yet as a society and as governments there is a huge amount of denial of what this might mean in terms of risk. Are we really being so smart? We have a collective fear of the effects of climate change on human society, because we can relate that to events we have seen before, such as floods, storms, droughts and extremes of temperature. There is a sense of reality around climate change and its possible outcomes, even though there is uncertainty and diversity of opinion. Do we have the same sense of reality around cyber risk? The Attributer will argue that we do not.

Let's first remember the definition of risk in SABSA terms, based on and wholly aligned with ISO 31000. Risk is the uncertainty of outcomes. There is likelihood of beneficial outcomes and damaging outcomes. The 'smart cyber world' opens up many opportunities, but what about the threats?

Since we always have incomplete information, we can never predict with a high level of confidence what the future will bring, unless we can be sure that it will look like the past. Experience shows that the future holds many surprises. We don't know what we don't know (Black Swan theory). The traditional statistical way to model risk is to develop a mathematical probability distribution and use the mean and standard deviation as predictors of extreme events, to a level of confidence that we find acceptable, and then prepare risk mitigation within that confidence interval. The data points for fitting a suitable distribution are things we have seen before – previous observations and current trends. Climate modelling follows this methodology.

Now consider the smart cyber world. The pace of development is fast and accelerating. We have almost no history of cyber events of significant scale on which to build a probability distribution. Worse than that, we have a history of how the world works in a non-cyber environment and we are using those event histories to model the future. Does anyone else see danger in this?

Take one thing on which the modern world depends: electricity. We have plenty of experience of localised power outages and how to deal with them. Weather events, seismic events, breakdowns of industrial relations, technology failure and many more are within our experience. However, smart cyber technology suggests that power outages on an altogether different scale are possible (even probable?). We are deploying smart grids, smart metering and other smart control systems to govern electricity supply and consumption. What would be the outcome of a widespread cyber attack on these systems? Consider an attack that would bring down the national electricity grids of several countries. Previous recovery strategies will not work. There will be no water or oil pumping, no telecommunications, no functional medical equipment, no road traffic control, no street lighting, no industrial production, just to mention a few of the impacts. Try to imagine a world without electrical power. Law and order would be at risk.

It is clear that enemies of the democratic world will use any means of attack at their disposal. The modern terrorist is smart, educated and cyber-competent. We must dispel the image of men with long beards and rifles living in caves in the mountains. Today's terrorists hide in plain sight, living amongst us and plotting sophisticated attacks that will do maximum damage to the democratic states they oppose. In the opinion of the Attributer, they are plotting and planning cyber attacks on a scale we have never before witnessed – data points that do not appear in our statistical models.

We need to shift into a different gear in our thinking and planning. The current approach of treating cyber-security as a technical problem with local technical solutions will not serve us if (when) this future unfolds. We need end-to-end, wall-to-wall thinking – the type of thinking that SABSA practitioners use in developing business and technology architectures.

The Attributer

VERSLAG CISO 6

EEN DISCUSSIE OVER SOC-SIEM

Op 16 september kwamen leden van het PvIB en GvRM traditiegetrouw bijeen voor een discussie over een onderwerp dat beide groepen interesseert. Dit keer ging het over Security Operations Centre (SOC) en Security Information and Event Management (SIEM). Ook voor deze bijeenkomst was Deloitte in Rotterdam weer gastheer waardoor de deelnemers tussen de bedrijven door van een ruim en onbelemmerd uitzicht konden genieten.

Bart van Staveren introduceerde de beide sprekers door te verwijzen naar de oorspronkelijke gedachte achter het onderwerp van deze middag, het tegenover elkaar stellen van de "zelfdoener" en de "uitbesteder" van SOC en SIEM. Hoe beoordeel je de risico's hiervan?

De "zelfdoener"

Kelvin Rorive, Productmanager Security bij Rabobank Nederland, liet het leerproces zien dat de Rabobank heeft doorgemaakt in het realiseren van een SOC dat gebruik maakt van de vele beschikbare informatie over alle invoer -en uitvoertransacties.

Het SOC van Rabobank functioneert als een interne bewaker van operationele risico's. SIEM moet daarbij behulpzaam zijn maar een SIEM als vergaarbak van logdata heeft snel het karakter van een ongerichte verzameling. Beter is het om gericht te werk te gaan, zo ondervond Rabobank. Daarom werden drie doelen gesteld: alertering, compliance reporting en forensisch onderzoek. Het verzamelen van data dient één van deze doelen te ondersteunen. Data-analyse ten behoeve van momenten waarop een aanval kan worden verwacht en het vroegtijdig herkennen van nieuwe dreigingen, is mogelijk als de data gericht verzameld is. Als basis van het verzamelen van data wordt een "usecase" gebruikt, een door de business gedefinieerde reden om data te verzamelen en te analyseren. Deze werkwijze is een prikkel voor de business om na te denken over risico's. Door deze aanpak wordt het SOC een faciliterende partij voor de business, zij kan vragen beantwoorden op grond van gericht verzamelde informatie. Usecases zijn gebouwd op basis van specifieke dreigingen waarvoor vervolgens rules worden gespecificeerd: 'als dit, dan dat'. Hierdoor ontstaan usecases met verschillende rules waardoor duidelijk wordt welke actie noodzakelijk is in specifieke gevallen. De data die wordt verzameld uit logbestanden wordt op deze manier betekenisvol.

De "uitbesteder"

Jan Terpstra, Senior Cyber Security Consultant HP Enterprise Security, ging in op het onderwerp Security monitoring. Door strubbelingen met de werkgever kon hij niet het oorspronkelijke verhaal houden. In plaats daarvan introduceerde hij de mogelijkheid security monitoring als service aan klanten aan te bieden. De behoefte aan security monitoring komt volgens Jan voort uit de ontwikkeling in het domein van de dreigingen, de druk van toenemende regelgeving en ontwikkelingen op het gebied van IT. Als voorbeeld kan de meldplicht datalekken gelden. Zijn ervaring is dat lekken vaak met grote vertraging bekend raken doordat niet het bedrijf zelf maar een derde partij het beheer voert. Daarom is het nodig en nuttig om beveiligingssystemen op datalekken voor te bereiden en medewerkers

bewust te maken. Ook Jan is van mening dat het belangrijk is vooraf te weten wat je met informatie uit SIEM wilt bereiken. Naast beveiligingssystemen zijn ook bewuste medewerkers nodig om hierbij te helpen.

Als leverancier van diensten gaat het Jan om de 'delivery capabilities'. Voor ieder mogelijk 'event' wordt bepaald welke correctieve actie nodig is. Bij de 'diagnose' door SIEM wordt dit meegenomen zodat er tijdens het event geen vragen gesteld behoeven te worden. Opmerkelijk zijn de getallen die HP noemt:

- 229 dagen voordat een inbreuk (gemiddeld) wordt opgemerkt
- 84% van de inbreuken gebeurd op et niveau van de applicatie
- 71% meer tijd kost het (ten opzichte van 2010) om een inbreuk op te lossen
- 94% van de inbreuken worden door een derde partij gemeld

Jan verhaalde over de expertise van HP op dit gebied en nam vervolgens enkele cases met ons door.

Discussie

Waar het gaat over gebeurtenissen valt al gauw het begrip: plannen maken. Zo ook tijdens CISO 6. Plannen worden gemaakt voor het geval dat. Vervolgens gaan de plannen de kast in om er niet meer uit te komen. Natuurlijk, een plan kan ook kort zijn, aansluiten op de praktijk, uitgaan van improvisatie en de alertheid en deskundigheid van medewerkers. Maar de twijfel blijft. Rabobank probeert voorbereid te zijn op incidenten (95% van de gevallen wordt binnen het SOC opgelost) en emergencies (5% van de gevallen en die worden overgedragen aan specifieke diensten). Veel van de voorbereiding hoort thuis in het ontwerpen en testen van de systemen.

SIEM kan worden opgevat als een brandmeldcentrale die (vroege) signalen oppakt en beoordeeld. SOC is de deskundige die kan interpreteren en besluiten kan nemen. Dat betekent dat SIEM goede informatie moet opleveren. Slechte informatie leidt immers tot slechte reacties van deskundigen.

Waarom zou je SIEM en/of SOC uitbesteden of juist zelf ter hand nemen? Jan meent dat de vraag naar managed services veelal komt uit organisaties die weten dat zelf niet te kunnen. Voor een bank kan gelden dat de schaalgrootte of de belangen zo groot zijn dat de eigen hand wordt geprefereerd. In beide gevallen geldt echter dat er grote schaarste is aan mensen die analyses kunnen maken die tot rules leiden. En ook hier de eeuwige vraag: "Hoe houd je het spannend en interessant voor dergelijke specialisten?" In beide gevallen geldt dat de kern van de SOC/SIEM-aanpak het inzicht in de processen is dat de gebeurtenissen en de mogelijke gevolgen kan duiden zodat de juiste data kan worden verzameld.

Het uitwisselen van informatie, waarschuwingen en ervaringen is vooral internationaal lastig door lokale verschillen in regelgeving.

De usecase moet altijd uit de business komen. Een voorbeeld: "Ik wil zeker weten dat alleen geautoriseerde gebruikers toegang hebben, dus als iemand ongeautoriseerd toegang probeert te krijgen dan …" Door Rabobank wordt data-analyse gebruikt om "het normale patroon" te vinden. Voor de afwijkingen zijn er dan de rules die de actie weergeven. Als bijvoorbeeld netwerk access control als preventieve maatregel wordt gebruikt om niet gevalideerde apparaten op het netwerk aan te sluiten, dan is dat een zaak van netwerkbeheer. Voor het SOC zijn alleen de afwijkingen van belang en wordt geen netwerk access control uitgevoerd.

SIEM wordt tegenwoordig breder getrokken in verband met cybersecurity. Criminologen, camera's, allerlei nieuwe mogelijkheden moeten worden benut om de nieuwe dreigingen bij te houden. Daarom is er grote behoefte aan "zachte informatie", waarbij predictive analysis ook nog vaak wordt tegengewerkt door regelgeving. Het gebruik van partners is nuttig maar de basisdata die als trigger dient moet wel goed zijn om samenwerking niet te frustreren.

Ook compliance kan vanuit het SOC worden ondersteund. Maar allereerst dienen goede usercases tot goede informatie te leiden. Het mengen van twee doelen tijdens de ontwikkeling van een SIEM leidt tot verwarring. Beter is eerst het ene en vervolgens het andere doel te realiseren.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuïteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB 8 boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals.Hij is bereikbaar via cees.coumou@planet.nl

Achter Het Nieuws

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

IS ER TOEKOMST VOOR DE SAFE HARBOUR-AFSPRAAK?

Met het arrest van het Europese Hof van Justitie is de Safe Harbour-afspraak tussen Brussel en Washington uit 1998 als intrinsiek onveilig beoordeeld, omdat de VS niet voldoen aan de kern van het recht op databescherming voor Europese burgers. Europese burgers mogen altijd inzage krijgen in hun gegevens en mogen die ook laten wijzigen of verwijderen. Het Hof oordeelt dat dit in de VS onvoldoende is gegarandeerd.

Veel Nederlandse bedrijven en organisaties maken gebruik van Amerikaanse cloudtoepassingen. Het Hof heeft bij het arrest tevens bepaald dat de privacytoezichthouders van de 28 lidstaten ieder apart bevoegd zijn er op toe te zien dat de rechten van hun burgers gerespecteerd worden, ook in de VS. Om grote economische schade te voorkomen en tegelijkertijd de rechten van de Europese burgers te beschermen moet er snel door de Europese Commissie en de 28 toezichthouders een nieuw raamwerk gemaakt worden voor Safe Harbour in nieuwe stijl. Wat zou er in dit raamwerk geregeld moeten worden en hoe zou het toezicht op naleving geregeld moeten zijn? Onze redacteuren geven hun mening.

Lex Dunn

Safe Harbour is dood, zoveel is ondertussen wel duidelijk geworden na de uitspraak van het Europese Hof. Maar wat nu? Er zijn talloze uitwisselingen van persoonsgegevens tussen bedrijven in Europa en Amerika, moeten die nu allemaal individuele Data Transfer Agreements gaan opstellen? En wat te denken van de grote spelers, zoals Microsoft, Facebook, Google? Allemaal Amerikaanse bedrijven met heel veel Europese gebruikers. Gelukkig lijkt het erop dat de EC wel onderkend heeft dat we eigenlijk niet zonder een soort Safe Harbour constructie kunnen, en wordt er dus nijver gewerkt aan een opvolger/vervanger. Zo'n nieuwe variant zal echter ook het onderliggende probleem niet oplossen: je kunt zoveel afspraken maken met Amerikaanse bedrijven als je wil, tot en met het


Lex Dunn


Lex Borger


Maarten Hartsuijker

ondertekenen in bloed toe, maar zolang de Amerikaanse overheid de wereld in twee kampen blijft verdelen (Amerikaanse staatsburgers met een redelijke mate van protectie, en de rest van de wereldburgers, die volkomen vogelvrij zijn) zal elke overeenkomst slechts "window dressing" zijn. En dan hebben we het nog niet eens gehad over wat Amerikaanse overheidsinstanties zoals de NSA nu al van ons Europeanen weten. Een pasklare oplossing heb ik ook niet, maar overweeg serieus of je (gevoelige) persoonsgegevens nog wel aan een Amerikaans bedrijf kunt/wilt toevertrouwen. Enne: lees vooral "Little Brother" van Cory Doctorow eens.

Maarten Hartsuijker

Amerikaanse cloudproviders zweren stuk voor stuk al jaren dat ze zich volledig aan Europese wet en regelgeving houden, maar zijn in eigen land ook verplicht de Amerikaanse wet na te komen. En helaas conflicteren die twee verantwoordelijkheden. Je kunt als bedrijf in Europa niet beloven de privacy van Europese klanten op Europese wijze te beschermen wanneer de overheid in eigen land je verplicht om die in stilte te schenden.

De Safe Harbour-uitspraak bevestigt wat de meeste beveiligings- en privacyspecialisten al jaren weten. Als je de privacy van je klanten volledig conform Europees recht wilt waarborgen, moet je geen data buiten de Europese Unie verwerken. En dat er door de uitspraak van het Europese hof nu naarstig naar een oplossing wordt gezocht zal daar vermoedelijk weinig aan veranderen. De belangen zijn zo groot dat er in de nieuwe afspraken onvermijdelijk clausules komen die het "onder bijzondere omstandigheden" of "in uitzonderlijke gevallen" mogelijk maken om de privacy van burgers te blijven schenden. Daar verbazen we ons dan over 10 jaar weer over.

Naar mijn mening is hier maar op één manier een einde aan te maken. Europa en de VS spreken af dat justitie en inlichtingendiensten alleen data vorderen van burgers uit hun eigen land. En dat een vordering die betrekking heeft op iemand met een andere nationaliteit altijd via de overheid van die persoon zal lopen. Alleen op die wijze kan ons land volledig haar eigen publieke belang dienen. En dat publieke belang zal dan soms, na het zorgvuldig toetsen van onze eigen wettelijke kaders, inhouden dat ons land gegevens zal verstrekken aan de Verenigde Staten.

Ondertussen heb je als organisatie bij het gebruiken van buitenlandse clouddiensten die veel operationele voordelen bieden een aantal belangrijke afwegingen te maken. Heb je bedrijfsgeheimen te beschermen die voor andere overheden van nationaal belang kunnen zijn? Wil je volledig voldoen aan Europese wet- en regelgeving? Accepteer je dat je met het volgen van de wet (bijvoorbeeld het hanteren van modelcontracten) vermoedelijk niet realiseert wat de wet heeft beoogd (beschermen van persoonsgegevens naar Europese maatstaven)? Past het verwerken van (persoons)vertrouwelijke informatie in een buitenlandse cloud bij de identiteit van de organisatie? Zal deze verwerking afbreuk doen aan het vertrouwen dat klanten in de organisatie stellen? Beantwoord dit soort vragen vooral op bestuursniveau en voorkom dat je als IT-afdeling risico's neemt die niet bij de organisatie passen.

Lex Borger

Misschien willen we wel te veel. Misschien pakken we het helemaal verkeerd aan. We proberen om de begrensde politieke wereld te projecteren op een inherent grenzeloos internet. Die grenzeloosheid en openheid is juist zo waardevol geweest voor de ontwikkeling van dit internet. En nu willen wij, Europa, het aan banden leggen. En de Verenigde Staten. En China. Enzovoorts.

Die grenzen in de politieke wereld zijn ook niet te bewaken. We zien dat niet alleen in de politieke onrust in de wereld van vandaag, maar ook in de moeite die we hebben om internationaal verkeer in de brede zin: mensen, diensten en goederen in 'goede' banen te leiden. We hebben afgesproken grenzen te respecteren, maar toch accepteren we eenzijdige verlegging daarvan, denk aan de annexatie van de Krim of de bezette gebieden door Israël, om twee dwarsstraten te noemen.

Wat maakt nu dat we denken dit goed te kunnen doen in het internet? Veel discussies gebruiken het woord 'vertrouwen', maar Safe Harbour is meer een uiting van wederzijds wantrouwen. En naar resultaten uit het verleden terecht. Wat we nodig hebben is om de macht naar onszelf toe te kunnen trekken. Laat ons zelf data versleutelen, of dit uitbesteden zoals we willen. Bemoei je daar niet mee als overheid en vraag zeker niet om een achterdeur. We weten hoe we dat moeten doen voor opslag en voor communicatie. Alleen nog niet voor verwerking. Laten we daar dan aan werken. Theoretisch moet het kunnen.

Ik ben realist genoeg om te weten dat dit een utopie is. Maar ik wilde graag even dromen...

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.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 2015
De abonnementsprijs in 2015 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

AUTOLEED

De laatste jaren is er meer en meer ingeslopen dat ons werk verder van ons huis afligt. Was het in de vorige eeuw nog redelijk normaal dat je de fiets pakte om naar je werk te gaan, tegenwoordig is een reistijd van meer dan twee uur geen uitzondering meer. Veel mensen kiezen voor de auto omdat het openbaar vervoer niet altijd even goed te gebruiken is. Vaak is de auto het meest ideale vervoermiddel, het filerijden wordt op de koop toe genomen of de overheid legt weer een strook extra asfalt neer om de toegenomen verkeersdrukte op te vangen. Op sommige plaatsen van het land liggen inmiddels tien banen naast elkaar - ik tel de vluchtstrook maar even niet mee.

Op die manier kan het verkeer opschieten. Om het milieu te sparen wordt de topsnelheid naar beneden gebracht en daardoor kunnen bewoners in de buurt van die wegen gewoon ademen en de was buitenhangen. Het zou natuurlijk nog mooier zijn als we de auto's die gebruik maken van die wegen ook schoner maken. Op die manier worden nu oude diesels uit een aantal binnensteden gemeden dit naar voorbeeld van onze Oosterburen. Een positievere actie is om zuinige auto's minder te belasten met BPM en andere belastingen en dat heeft effect. Het Nederlandse wagenpark verandert aanzienlijk, de gemiddelde lengte van de auto's halveert en bij ieder tankstation verschijnt een ruimte waar de elektrische auto's opgeladen kunnen worden.

Ik tank zelf gewoon diesel en tijdens het tanken kijk ik wat rond en zie tot mijn verbazing nooit een auto bij de laadpalen staan. Wat ik wel merk is dat de auto's om mij heen zuiniger en zuiniger worden, de één kan wel 1 op 30 rijden en de andere is ongelofelijk schoon. De 1 op 30 heb ik, ondanks de beloften van de fabrikant, jammer genoeg nog nooit weten te halen met de auto van mijn vrouw. Maar 1 op 15 is ook mooi. De uitstoot is natuurlijk eenvoudig te meten, je zet de auto aan de computer en je meet de CO_2-uitstoot. Zeer eenvoudig en hierdoor is het ook erg makkelijk te bepalen hoeveel BPM en bijtelling betaald moet worden. Iedereen blij, de autowereld komt helemaal op de kop te staan, populaire merken zijn ineens niet meer populair en merken waar men vroeger niet naar omkeek zijn niet aan te slepen.

De kopers die zuinige auto's hebben gekocht protesteren wel als ze merken dat de auto's niet echt zo zuinig zijn, maar op basis van de Europese regels mogen fabrikanten wel hele zuinige auto's beloven maar hoeven ze niet te worden geleverd. CO_2 meten kun je niet als je de apparatuur niet hebt. Dat hoeft ook niet, want iedere auto die wordt toegelaten op de Nederlandse weg wordt natuurlijk gekeurd.

Totdat we erachter komen dat sommige fabrikanten eigenlijk helemaal geen schone auto's leveren, maar slimme programmeurs in dienst hebben die het doen lijken of de auto's schoon zijn. Miljoenen auto's die verkocht worden aan berijders die daardoor voordeel hebben met lagere belastingen. Eerst alleen diesels met een redelijk kleine motor, nu ook de grote diesels en ook de benzineauto's blijken niet helemaal conform specificaties te functioneren. Ik heb het hier wel eerder genoemd: perverse winstdrang en je niet druk maken om de wereld om je heen. Klagen dat de uitstooteisen te hoog liggen, zodat die vervolgens door de Europese Unie worden verruimd. Voordat we het weten rijden we weer in de smerige diesels rond die nu geweerd worden in sommige binnensteden.

Miljarden zijn door de put gespoeld omdat deze aan subsidie werd uitgegeven aan auto's die het niet verdienden. Mijn automerk is gelukkig wel altijd eerlijk met betrekking tot uitstootcijfers of ben ik nu een beetje naïef?

Berry

PRIVACY THE NEXT BIG THING!

De Security Academy presenteert een tweetal geheel nieuwe privacy opleidingen die zowel de nieuwe Europesche als de nationalte wet- & regelgeving behandelen. Beide opleidingen worden in 2016 door het EXIN geaccrediteerd en geëxamnineerd. U heeft hiermee dus een onafhankelijke, internationaal erkende certificering op zak.

Privacy Foundation

Maak in drie dagen grondig kennis met de Nederlandse en Europese wet- en regelgeving op het gebied van privacy.

Deze cursus is uniek omdat er een voor "gewone" medewerkers (lees anderen dan juristen) begrijpelijke en praktische vertaling wordt gegeven van de relevante wet- en regelgeving. Aan de hand van veel praktijkvoorbeelden vergaart u voldoende kennis en inzicht om adviezen te kunnen geven over privacyvraagstukken binnen uw organisatie. Na deze cursus kunt u als gesprekspartner optreden voor de diverse (management)lagen binnen uw organisatie en voor derden buiten uw organisatie.

Er gelden geen specifieke toelatingseisen om deel te kunnen nemen aan de cursus Privacy Foundation. Na voltooiing van de cursus bent u klaar om deel te nemen aan het examen "Privacy Foundation" van EXIN. EXIN verwacht dit examen begin 2016 aan te gaan bieden.

Prijs: € 1.950,- exclusief BTW

Privacy Advanced

Deze cursus is een vervolg op de Privacy Foundation cursus. In deze drie daagse cursus wordt ingegaan op de zaken die binnen uw organisatie geregeld dienen te worden om aan de eisen die het College stelt te voldoen.

Deze cursus is bedoeld voor iedereen die in zijn werk verantwoordelijk is voor de inrichting, aansturing of controle van de manier waarop met persoonsgegevens wordt omgegaan. U leert daadwerkelijk de pricvacywetgeving te implementeren binnen uw organisatie.

Om optimaal rendement uit deze cursus te kunnen halen wordt aangeraden dat u eerst deel hebt genomen aan de cursus "Privacy Foundation". Indien u al beschikt over een gedegen kennis van de relevante wet- en regelgeving op het gebied van privacy is dat ook voldoende.

Prijs: € 1.950,- exclusief BTW

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL