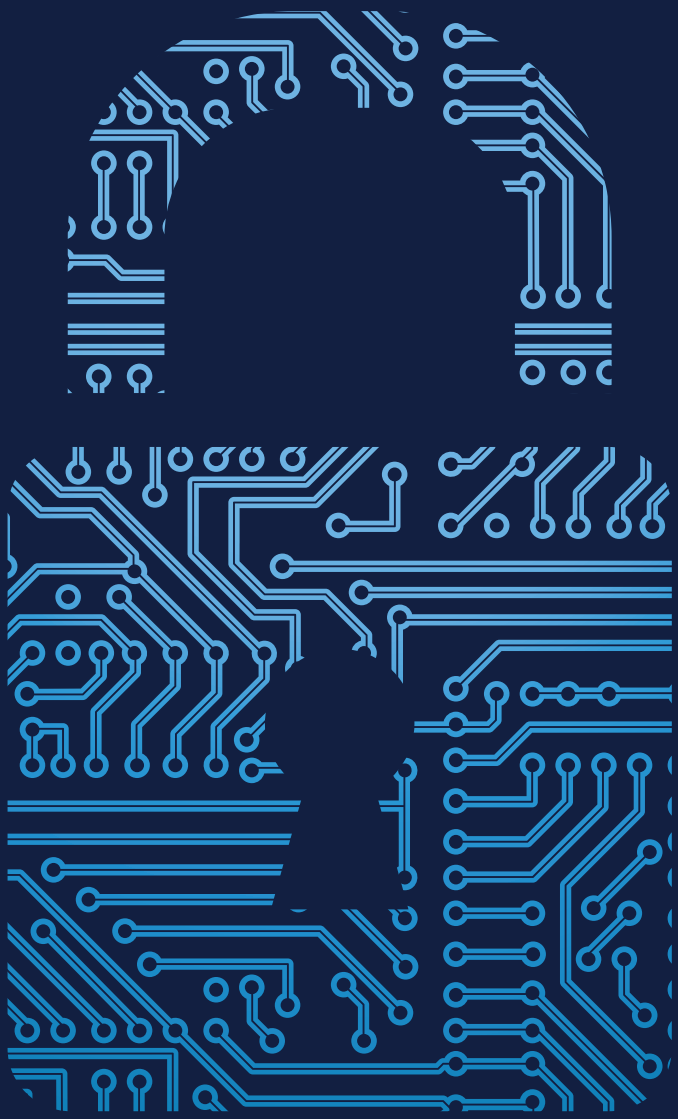
iB
INFORMATIEBEVEILIGING
jaargang 16 - 2016
#2



PRIVACY EN AUTHENTICATIE

Meldplicht Cybersecurity voor een veiligere samenleving?

eIDAS betrouwbaarheid

Polymorfe pseudonimisering

Let's Encrypt is in Public Beta

SECURITY Academy

Unlock je carrièrepad bij de Security Academy

Studeren aan de Security Academy staat voor diepgang en kwaliteit. Voor zowel de security specialist als de business continuity en crisismanager bieden wij 28 certificeringen aan waarmee u zich, ongeacht uw instapniveau, verder kunt ontwikkelen. Benieuwd naar ons geheel vernieuwde certificeringsprogramma? In mei vindt de officiële lancering plaats van het Security Academy Certification Program.

*Ga voor een sneak preview naar de **Security Academy Backstage FB** pagina*

SecurityAcademy.nl

info@securityacademy.nl

+31(0)348-408061

THEMA: PRIVACY EN AUTHENTICATIE

Ik heb getwijfeld of we van het thema 'privacy versus identiteit' moesten maken. Dat klonk echter nietszeggend. Waarom? Het internet is een hooiberg waar je anoniem kunt zijn, maar waar je soms je identitieit bekend wilt maken of moet maken. Maar anonimiteit is geen privacy. Authenticatie houdt een garantie van identiteit in, privacy is alleen mogelijk met een garantie van anonimiteit. Dus privacy en authenticatie zijn twee gelijkwaardige kwaliteiten die cruciaal zijn op onze tochten over het internet. Net als bij gebrek aan authenticiteit een identiteit zo goed als waardeloos is, is bij gebrek aan privacy anonimiteit zo goed als waardeloos. Toch is er een groot verschil: voor identiteiten en authenticatie hebben we standaarden, zoals de eIDAS. Vier niveaus van authenticatie, praktisch toepasbaar op vele mechanismen. Voor anonimiteit en privacy hebben we encryptie, ook geregeld in standaarden, heel krachtig. De heren achter de protocollen RSA (Rivest, Shamir en Adleman) en DH (Diffie en Hellman) hebben allen de Turingprijs gewonnen (2002 en 2015).

Zó krachtig is encryptie, dat politici ons graag willen laten geloven dat het goed is om jouw privacy in te ruilen voor jouw veiligheid. Vertrouw maar op de veiligheid die de overheid biedt... Maar waarom moet ik mijn privacy inleveren om veilig te zijn? In de fysieke wereld leveren alleen criminelen en verdachten hun privacy in, en die laatsten pas na rechterlijke toetsing. Ik heb geen last van een huiszoeking bij een verdachte, tenzij ik er direct bij betrokken ben.

Nu we toch aan het vergelijken zijn: wat is het elektronische equivalent van een huiszoeking doen? Een encryptiesleutel krijgen? Nee. Ik heb een paar huiszoekingen ingeleid zien worden met het openrammen van een deur, en niet het overhandigen van de sleutel. In encryptietermen: een brute-force attack. Bij een gemiddelde voordeur is dat iets wat een paar seconden duurt. Een zware kluisdeur openbreken vereist ander materiaal en duurt een paar dagen, maar ook dat klusje krijgt de politie (met gerechtelijk bevel) geklaard.

Encryptie breken is echter anders: dat duurt geen seconden, of dagen. Dat duurt duizenden of miljoenen jaren in het geval van een brute-force attack. En dáár wringt de schoen: het inbreken is niet meer zo simpel als toestemming krijgen van de rechter voor een gerichte brute-force aanval. Er moeten creatief gedaan worden, gebruik gemaakt worden van implementatie-fouten of backdoors (FBI versus Apple). Dit verhaal is nog lang niet af.

In dit nummer wat over authenticatiemechanismen, privacy en encryptie. Groot goed, wat we allemaal in ere moeten houden.

Happy reading.

Lex Borger, hoofdredacteur

In dit nummer

PRIVACYBESCHERMING IN HET ELEKTRONISCHE ONDERWIJS GEBASEERD OP POLYMORFE PSEUDONIMISERING

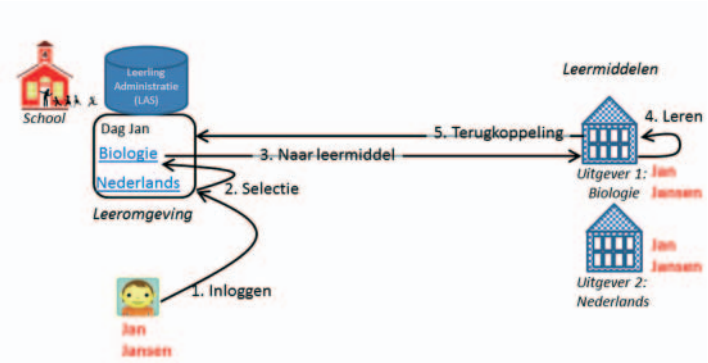
Samenvatting

In [1] wordt een elektronisch identiteitstelsel beschreven dat de Nederlandse overheid wil inzetten in de onderwijssector. Dit stelsel maakt het mogelijk om leerling gegevens uit te wisselen tussen scholen en private partijen, namelijk de uitgevers van elektronische boeken (e-boeken). Het stelsel introduceert in feite drie nieuwe "BSNs" (persoonsnummers) binnen het onderwijs die worden gedeeld met deze private partijen. In dit artikel wordt allereerst beargumenteerd dat deze opzet onvoldoende recht doet aan het dataminimalisatiebeginsel zoals vastgelegd in privacywetgeving [2]. Vervolgens wordt een privacyvriendelijk alternatief beschreven waarvan de cryptografische details in [3] staan beschreven. Dit alternatief neemt wel het dataminimalisatie beginsel in acht en geeft leerlingen en hun ouders controle over gegevens uitwisselingen.

Het alternatief is gebaseerd op zogenaamde polymorfe pseudonimisering en dit artikel legt de cryptografische principes hierachter uit alsmede de functionele toepassing ervan. Het betreft een privacy enhancing technologie die in 2014 is ontwikkeld binnen de Nederlandse overheid voor gebruik binnen het nationale eID-stelsel, eID2.0 genaamd. Zie [4] en de presentatie die hierover is gegeven tijdens de PvIB-cryptonacht [5] op 10 februari 2015. Binnen de voorgestelde opzet is een leerling bekend bij een partij onder een pseudoniem dat ook specifiek voor deze partij is. Een partij kent ook alleen het eigen pseudoniem van een leerling en niet dat bij een andere partij. Dit geldt ook voor de scholen. Indien noodzakelijk is privacyvriendelijke koppeling tussen partijen echter wel mogelijk. Uitgevers kunnen bijvoorbeeld testresultaten van een leerling naar diens school sturen waarbij verschillende uitgevers niet in staat zijn vast te stellen of het dezelfde leerling betreft. De polymorfe opzet lijkt eenvoudig toepasbaar in combinatie met vaak toegepaste SAML-standaard. De technologie vormt ook een basis voor aanvullende privacyvriendelijke diensten zoals een inzage dienst waar gebruikers (onder pseudoniem) kunnen zien wat er over hen is vastgelegd en uitgewisseld. Een verdere uitbreiding (polymorfe versleuteling) maakt het mogelijk om leerlinggegevens versleuteld bij een cloud-provider te plaatsen. Hoewel deze cloud-provider geen toegang heeft tot deze gegevens is hij wel in staat deze onder condities toegankelijk te maken voor partijen voor wie dat noodzakelijk is. De polymorfe encryptie en pseudonimisering (PEP) technologie maakt ook interessante toepassingen in andere sectoren mogelijk, bijvoorbeeld in de zorg of in de justitiële keten. Bij de Digital Security-groep van de Radboud Universiteit wordt op dit moment gewerkt aan een implementatie van deze opzet binnen de zorg.

Inleiding

De beschrijving van Nederlandse e-leerboeken is enigszins versimpeld om reden van toegankelijkheid. Specifiek wordt de bemiddelende rol van distributeurs tussen scholen en uitgevers niet beschreven. Distributeurs vormen een verdere privacyuitdaging in het onderwijs. De geschetste toepassing van polymorfe pseudonimisering in dit artikel kan echter eenvoudig worden uitgebreid met distributeurs.



Figuur 1 - Werking e-leerboek

Scholen zijn conventionele leerboeken aan het vervangen door hun elektronische evenknieën, elektronische leerboeken, of kortweg e-leerboeken. De term is wat misleidend, omdat een e-leerboek veel meer functionaliteit omvat dan een gewoon leerboek. Een e-leerboek maakt rijkere inhoudsvormen vormen mogelijk zoals audio en video. Het maakt ook interactie met de leerling mogelijk waaronder oefeningen rond de leerstof. Daarbij kan het de leraar inzicht geven in de vooruitgang van een

Dr. Eric Verheul CISA CISSP is deeltijd hoogleraar binnen de Digital Security-groep van de Radboud universiteit. Hij geeft een mastercollege over securitymanagement gebaseerd op ISO27001 en doet onderzoek naar cryptografische toepassingen waaronder voor privacybescherming. Daarnaast is Eric zelfstandig consultant en auditor op het gebied van informatiebeveiliging, cryptografie en privacy. Vanuit deze hoedanigheid is hij ook betrokken bij Idensys (voorheen eID-Stelsel). Dit artikel is geschreven op persoonlijke titel. Eric is bereikbaar op eric.verheul@keycontrols.nl of eric.verheul@cs.ru.nl

leerling waarbij deze de leerling aanvullende taken kan geven. Een e-leerboek heeft typisch de vorm van een website bij een uitgever. Om toegang te krijgen tot zijn e-leerboek moet de leerling (Jan Jansen in figuur 1) eerst inloggen (Stap 1) op het portaal van de school waarop de diverse e-leerboeken worden gepresenteerd met weblinks (URLs). Na klikken op een dergelijke link (Stap 2) wordt de leerling doorgestuurd (redirected) naar het e-leerboek bij de uitgever (Stap 3) waar hij de leerstof tot zich kan nemen (Stap 4). Periodiek levert de uitgever terugkoppeling aan de school over Jan Jansen (Stap 5), bijvoorbeeld met testresultaten.

Binnen de werking van een e-leerboek is herkenning van de leerling door school en de uitgever essentieel. Na een eerste gebruik door de leerling stuurt de uitgever een verzoek naar de school om te betalen voor diens licentie. Deze eerste use-case illustreert het belang dat de leerlingidentiteit bij de uitgever door hem kan worden gekoppeld aan de leerlingidentiteit bij de school. In essentie bestaat de leerlingidentiteit bij de school uit diens Burgerservicenummer (BSN). Een tweede use-case is dat het schoolportaal de leerling moet kunnen doorsturen naar diens e-leerboek bij de uitgever. Dit illustreert het belang van de omgekeerde koppeling, i.e. dat de identiteit van de leerling bij de school door hem kan worden gekoppeld aan de identiteit bij de uitgever. Een derde use-case is dat de uitgever feedback geeft aan de school, bijvoorbeeld testresultaten. Vanuit identiteitmanagement is dit vergelijkbaar met de eerste use-case. Een laatste use-case is dat als een leerling naar een andere school verhuist zijn identiteit bij uitgevers ongewijzigd blijft om het verlies van historische gegevens te vermijden. Dat wil zeggen, als Jan Jansen vanaf een ander schoolportaal naar dezelfde e-leerboek uitgever zou gaan, dan moet hij op hetzelfde account (identiteit) terechtkomen bij de uitgever.

Op dit moment wordt bij het Nederlandse e-leerboek veelal het eenvoudigst mogelijke identiteitstelsel toegepast. Daarbij wordt door de school de volledige naam van de leerling, en klas doorgegeven aan de uitgever. In opzet maakt dit de drie use-cases eenvoudig mogelijk, hoewel de toepassing in de vierde use-case (schoolverhuizing) wat foutgevoelig is omdat namen niet uniek zijn. Hoewel deze opzet functioneel dus voldoet is hij niet conform de privacywetgeving. Dit omdat de uitgever de leerlingidentiteit niet hoeft te kennen, net zo min als een uitgever van papieren boeken dat hoeft. Specifiek is de huidige opzet in strijd met het dataminimalisatiebeginsel uit de concept Europese privacyverordening [2]: "persoonsgegevens moeten adequaat en ter zake dienend zijn en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt; zij worden alleen verwerkt wanneer en voor zolang als de doeleinden niet zouden kunnen worden verwezenlijkt door het verwerken van andere gegevens dan persoonsgegevens". Daarbij merken wij nog op dat naast de identiteit informatie ook de aard van het e-leerboek en de testresultaten privacy gevoelig kunnen zijn. Deze kunnen immers duiden op dingen die een leerling zijn overkomen zoals mishandeling of misbruik of wijzen op (medische) aandoeningen zoals dyslexie of dyscalculie. Dit soort informatie kan commercieel worden misbruikt om leerlingen in hun verdere leven mee te profileren, lees: mee te achtervolgen. Het is niet voor niets dat dit soort informatie bekend staat als bijzondere persoonsgegevens waarvan de privacyverordening speciale behandeling vereist. Bovenstaande discussie toont aan dat het niet acceptabel is dat uitgevers over de volledige identiteiten van leerlingen mogen beschikken.

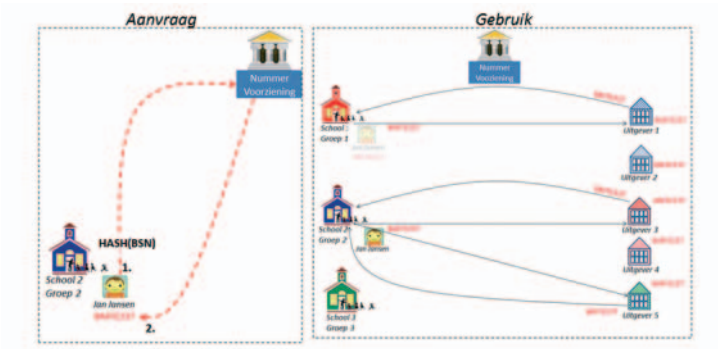
Leeswijzer

- In dit artikel bespreken wij eerst in punt 3 het identiteit stelsel [1] dat de Nederlandse overheid wil inzetten in de onderwijssector en dat een betere privacybescherming beoogt dan het huidig toegepaste stelsel. Daarbij zullen wij betogen dat ook dit stelsel nog onvoldoende recht doet aan het dataminimalisatiebeginsel.
- Vervolgens bespreken we in punten 4, 5, 6 een alternatief identiteitstelsel gebaseerd op polymorfe pseudonimisering beschreven in [3]. Daarbij worden in punt 4 eerst de principes achter polymorfe pseudonimisering uitgelegd die vervolgens in punt 5 worden toegepast in een alternatief identiteitstelsel. Punt 6 gaat in op de beveiliging en privacybescherming van dit stelsel.
- Punt 7 gaat kort in op de implementatie van de polymorfe opzet binnen SAML-implementaties.
- Punt 8 beschrijft een tweetal uitbreidingen op dit stelsel: privacyvriendelijke attribuutdiensten en een centrale inzagedienst.
- Punt 9 tenslotte, beschrijft de gebruikte verwijzingen.

De opzet van sectorpseudoniemen

In [1] wordt een verbeterd identiteitstelsel beschreven dat tegen moet gaan dat nog volledige leerlingidentiteiten moeten worden verstrekt aan uitgevers. Daarbij wordt het onderwijs onderverdeeld in drie sectoren: primair onderwijs (po), voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo). Een sector omvat alle scholen en de uitgevers die daarbinnen actief zijn. Daarbij is een leerling binnen een sector bekend onder een sectorpseudoniem dat cryptografisch gebaseerd is op het BSN-nummer van de leerling. Een school kan het sectorpseudoniem aanvragen bij een centrale partij, Nummervoorziening genaamd. Zie de linkerkant van figuur 2. Hiertoe dient de school het BSN in gehashde vorm op te sturen naar de Nummervoorziening. Deze zet dit om naar het sectorpseudoniem door de hash te versleutelen met een

geheime symmetrische sleutel en retourneert dit naar de school. Bij alle communicatie in de sector over de leerling wordt vervolgens het sectorpseudoniem opgenomen. Zie de rechterkant van figuur 2. Het toepassen van de hash operatie voegt overigens niet veel beveiliging toe omdat het BSN eenvoudig kan worden herleid uit zijn hash door middel van een bruteforce-aanval. In [1] wordt de eufemistische term ketenpseudoniem gebruikt omdat (pagina 20) het pseudoniem afhankelijk kan zijn van een "keten" van partijen in een sector. Op pagina 11 van [1] wordt echter expliciet opgemerkt dat hetzelfde pseudoniem voor alle partijen binnen een sector gebruikt wordt. Dit kan ook worden afgeleid uit de eigenschap op pagina 6 van [1] dat het pseudoniem ongewijzigd blijft als een leerling naar een andere school verhuist (die van andere uitgevers gebruik kan maken). Hoewel praktisch worden met de sectorpseudoniemen dus feitelijk drie nieuwe persoonsnummers geïntroduceerd. In dat licht is de term sector persoonsnummer eigenlijk meer op zijn plaats voor ketenpseudoniem dan sectorpseudoniem. Dit is evenwel de term die wij als compromis zullen gebruiken in dit artikel.



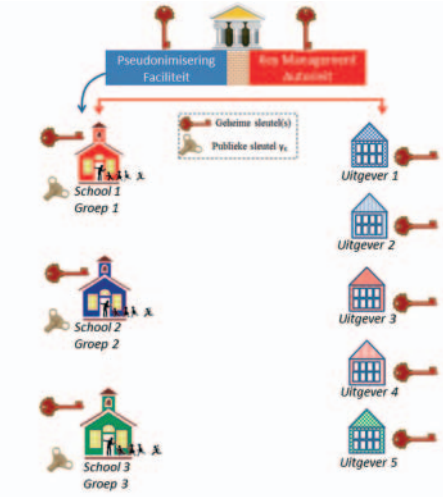
Figuur 2 - Werking sectorpseudoniemen

Wij menen dat ook de sectorpseudoniem variant conflicterend is met het dataminimalisatiebeginsel uit de Europese privacyverordening. Immers, de sectorpseudoniemen stellen uitgevers in staat hun databases te koppelen hetgeen niet alleen onnodig, maar ook onwenselijk is. Uitgevers kunnen aldus samenwerken om hun data te combineren en zo ook leerlingen te identificeren. Meer zorgwekkend is dat partijen (scholen, uitgevers) gehacked kunnen worden en waarbij de koppeling en identificatie door de hackers wordt uitgevoerd. Het resultaat kan worden misbruikt, verkocht of zelfs worden gepubliceerd als onderdeel van een chantage. Twee min of meer willekeurige incidenten onderstrepen dit gevaar. De hack in de zomer van 2015 op het Amerikaanse Office of Personnel Management [6], toch niet de eerste beste partij, leidde tot een compromittatie van meer dan 22 miljoen persoonsgegevens waaronder van CIA-medewerkers. De hack op de 'overspelsite' Ashley Madison [7], ook in de zomer van 2015, leidde tot de compromittatie van meer dan 37 miljoen persoonsgegevens. Hierbij werden de persoonsgegevens ook gepubliceerd nadat een chantagepoging mislukte. De indeling in drie sectoren in [1] is bedoeld als een rudimentaire privacymaatregel maar hindert ook de doelstelling van het ontwerp: noodzakelijke gegevensuitwisseling in het onderwijs. Immers, wanneer een leerling van type onderwijs verandert (bijvoorbeeld van PO naar VO) dan is het niet meer mogelijk om de gegevens van de leerling nog te koppelen zelfs als dat wel gewenst is, e.g. bij continue dyslexietesting. De opzet die wij in de volgende secties beschrijven, is niet gebonden aan sectoren en maakt elke noodzakelijke koppeling van gegevens tussen partijen mogelijk.

Principes van polymorfe pseudonimisering

Binnen de opzet van de polymorfe pseudonimisering (PP) bestaan naast deelnemers (i.e. scholen en uitgevers) ook twee Trusted Third Parties:

- een Key Management Authority (KMA) die verantwoordelijk is voor het beheer van cryptografische sleutels en de distributie daarvan aan de deelnemers en de Pseudonimisering Faciliteit.
- een Pseudonimisering Faciliteit (PF) die scholen helpt met het verstrekken van pseudoniemen aan uitgevers.

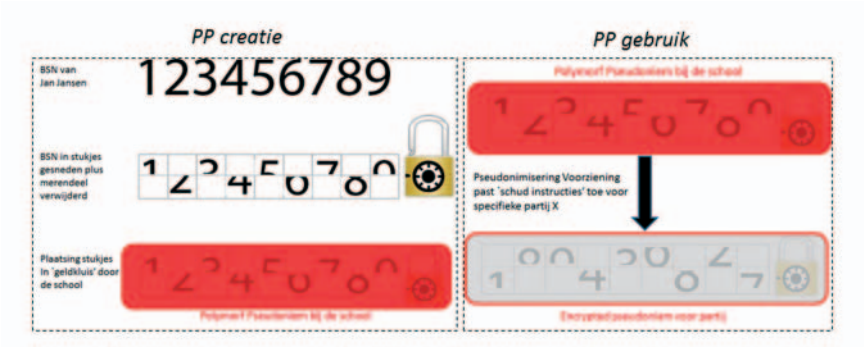


Figuur 3 - De polymorfe infrastructuur

Zie figuur 3. Het is belangrijk dat de KMA en de PF van elkaar gescheiden zijn. De basis van polymorfe pseudonimisering is dat de KMA een systeemwijde publieke sleutel yK genereert en die aan de scholen verstrekt. Het gebruikte publieke sleutelsysteem is evenwel niet het bekende RSA-systeem maar het ElGamal-systeem [8] gebaseerd op elliptische kromme cryptografie. Dit systeem is zelfs nog ouder dan het bekende RSA-publiekesleutelsysteem en is sterk verbonden met het bekendere Diffie-Hellman-sleuteluitwisselingsysteem. Het

bijzondere van de publieke sleutel yK is dat de bijbehorende private sleutel xK door niemand wordt gebruikt om berichten mee te ontsleutelen; dit wordt later duidelijk. De KMA genereert ook ElGamal publieke sleutelparen voor de deelnemers en verstrekt die aan hen. Deze sleutelparen zijn cryptografisch verbonden aan de publieke sleutel yK; dit wordt in [3] beschreven.

Om een leerling op te nemen in de PP-infrastructuur versleutelt de school een hash van diens BSN met de publieke sleutel yK. Dit heet het polymorfe pseudoniem van de leerling: het is wel gebonden aan de leerling middels diens (gehashte) BSN maar nog niet aan een deelnemer. Een polymorf pseudoniem is dus een ElGamal-versleuteling van een BSN-hash. Het berekenen van een dergelijke hash kan vergeleken worden met het in kleine stukjes snijden van een afgedrukt BSN waarbij het merendeel van de stukjes volgens een vaste methode wordt verwijderd. Daarmee blijft wel een soort unieke vingerafdruk over waaruit je het oorspronkelijke BSN niet meer kunt herkennen. Publieke versleuteling van de BSN-hash kan worden vergeleken met het plaatsen van de overgebleven stukjes in een geldkistje en deze op slot doen met een (open) hangslot waarvan je de combinatie niet bezit. Zie figuur 4. Na sluiting van het hangslot kan alleen de persoon met die combinatie het geldkistje dan nog openen. In onze situatie is dit dus de private sleutel xK. ElGamal-versleuteling heeft drie fraaie wiskundige eigenschappen die we aan de hand van de geldkistje-metafoor kunnen uitleggen. Zie Propositie 2.1 in [3].



Figuur 4 - Opzet polymorfe pseudonimisering

A. De eerste eigenschap is dat je door wiskundige bewerkingen op het reeds versleutelde bericht de ontsleutelde boodschap gericht kunt beïnvloeden, i.e. de boodschap die de sleuteleigenaar zal aantreffen na opening van het kistje. Dit is goed voorstelbaar in de geldkistje-metafoor. Als iemand het geldkistje gaat schudden dan zullen de overgebleven stukjes papier waarop het BSN stond afgedrukt anders worden gerangschikt. Het is die nieuwe rangschikking die de eigenaar van de sleutel zal aantreffen bij opening van het geldkistje met zijn combinatie. Merk ook op dat de persoon die het geldkistje heeft geschud geen idee heeft wat het eindresultaat is geworden.
B. De tweede eigenschap is iets ingewikkelder voor te stellen maar dit komt er op neer dat door schudden er ook voor kan worden gezorgd dat de combinatie waarmee het geldkistje kan worden geopend verandert. Waar het oorspronkelijke geldkistje alleen met de KMA-sleutel xK kan worden geopend kan het geldkistje na schudden alleen nog met een andere sleutel worden geopend.
C. De derde eigenschap, randomisatie, is weer goed uit te leggen in de metafoor. Dit komt erop neer dat iedereen betrokken bij het transport van het geldkistje dit een ander kleurtje kan verven zodat een geldkistje niet te volgen is. In de metafoor: het kistje gaat blauw in de bestelbus van de koerier en komt er rood uit. Net zoals iedereen een geldkistje kan verven, kan ook iedereen de randomisatie uitvoeren.

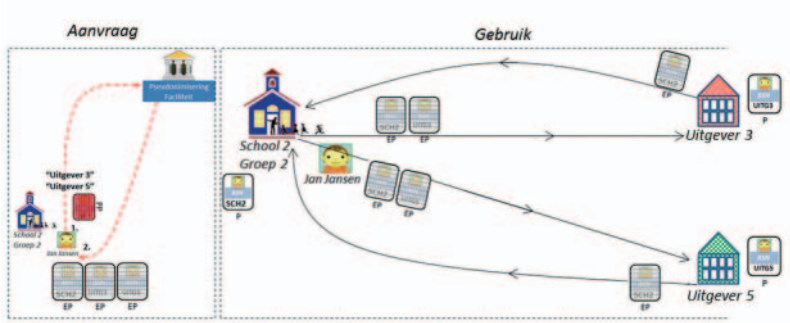
Het idee is nu dat de Pseudonimisering Faciliteit van de KMA geheim sleutelmateriaal krijgt om bovenstaande operaties A. en B. uit te voeren en vervolgens operatie C. uit te voeren. Dat wil zeggen dat de Pseudonimisering Faciliteit door 'gericht schudden' (en verven) een polymorf pseudoniem van een leerling kan omzetten in een encrypted pseudoniem van de leerling voor een specifieke partij. Alleen deze partij kan het pseudoniem hieruit herleiden; het pseudoniem is daarbij ook specifiek voor de leerling bij de partij. Bij een andere partij heeft de leerling een ander pseudoniem. De crux is nu dat een encrypted pseudoniem het mogelijk maakt om te verwijzen naar een persoon (pseudoniem) bij een andere partij, zonder deze te kennen. Zoals we zullen zien in de volgende sectie maakt dat privacyvriendelijke uitwisseling van persoonsgegevens mogelijk.

Toepassing van polymorfe pseudonimisering in het onderwijs

De toepassing van polymorfe pseudonimisering is nu als volgt, vergelijk figuur 5. Voor elke leerling die e-leerboeken nodig heeft, maakt de school een polymorf pseudoniem met de publieke sleutel yK. De school stuurt dit polymorfe pseudoniem van de leerling naar de PF samen met de namen van de e-leerboekuitgevers. Zie stap 1 in de linkerkant van figuur 5; hier is sprake van twee uitgevers. De PF zet dit dan met het sleutel materiaal om naar een encrypted pseudoniem van de leerling bij deze uitgever. Deze is dus alleen te onsleutelen door de bedoelde uitgever en bevat het pseudoniem van de leerling

dat specifiek voor de uitgever is. De school krijgt behalve de uitgever encrypted pseudoniemen ook een encrypted pseudoniem van de leerling bij de school zelf. Zie stap 2 in de linkerkant van Figuur 5. De school kan hieruit het pseudoniem ontsleutelen. Dat wil zeggen de leerling is bij de school zowel bekend onder zijn BSN als onder een schoolspecifiek pseudoniem.

Met deze opzet kunnen we nu eenvoudig de vier use-cases uit punt 2 bedienen. Vergelijk de rechterkant van figuur 5. Bij het eerste gebruik van een e-leerboek door een leerling stuurt de school zowel het encrypted pseudoniem van de leerling bij de uitgever als dat van de school zelf mee. Uit het eerste kan de uitgever het pseudoniem afleiden waarmee hij voortaan de leerling kan herkennen zoals vereist in de tweede use-case. Om te zorgen dat de school betaalt voor de e-leerboeklicentie, i.e. de eerste use-case, stuurt de uitgever een factuur aan de school met daarop het encrypted pseudoniem van de leerling van de school. De school kan hieruit het pseudoniem van de leerling bij de school afleiden en zo bepalen dat het betalingsverzoek terecht was. Als de uitgever de testresultaten over de leerling wil verstrekken aan de school (derde use-case) dan kan dat ook door het encrypted pseudoniem van de leerling bij de school mee te geven. Dit is vergelijkbaar met de afhandeling van de factuur door de school. Tot slot, doordat alle scholen dezelfde publieke sleutel yK gebruiken, is het pseudoniem bij een uitgever onafhankelijk van de school. Dat wil zeggen dat ook aan de vierde use-case wordt voldaan.



Figuur 5: Toepassing van polymorfe pseudonimisering

Beveiliging en juridische conformiteit

In Propositie 4.1 van [3] worden de volgende cryptografische claims bewezen rond polymorfe pseudonimisering. Deze zijn alle gebaseerd op bekende beveiligingseigenschappen van het ElGamal-systeem:

- Uitgevers zijn niet in staat om hun pseudoniemen te koppelen met BSNs van leerlingen of deze hieruit af te leiden.
- Samenspannende uitgevers zijn niet in staat om hun pseudoniemen onderling te koppelen.
- Scholen zijn niet in staat om de pseudoniemen bij uitgevers te bepalen, deze te koppelen met BSNs van leerlingen of om pseudoniemen van partijen te koppelen.
- Afluisterende partijen zijn niet in staat om leerling gegevens uitwisselingen te koppelen op basis van polymorfe of encrypted pseudoniemen die worden meegestuurd.
- De Pseudonimisering Faciliteit krijgt geen informatie over de activiteiten van leerlingen, en is niet in staat om pseudoniemen te koppelen met BSNs of pseudoniemen van partijen te koppelen.

De eerste drie claims zijn verbonden met een wiskundig hard probleem dat bekend staat als het Diffie-Hellman-beslissingprobleem (decisional Diffie-Hellman problem). Zie [9]. De vierde claim staat ook wel bekend onder de semantische veiligheid van het ElGamal-encryptiesysteem, vergelijk Theorem 10.20 in [9]. De laatste claim volgt uit deze semantische veiligheid gecombineerd met het feit dat de BSN-hash versleuteld wordt gestuurd naar de Pseudonimisering Faciliteit onder een publieke sleutel waarvan deze faciliteit het private gedeelte niet heeft. Het College Bescherming Persoonsgegevens, dat sinds het begin van 2016 Autoriteit Persoonsgegevens heet, heeft in [10] een richtlijn gepubliceerd over pseudonimisering gebruik makend van een Trusted Third Party. Als aan de vereisten in de richtlijn wordt voldaan dan worden de resulterende pseudoniemen niet beschouwd als persoonsgegevens. Toegepast in onze context betekenen deze vereisten dat vakkundig gebruik moet worden gemaakt van cryptografische technieken en dat de verantwoordelijke voor de identificerende data, i.e. de school, alleen een secure-hash van het BSN naar de pseudonimisering faciliteit mag sturen. De bewijzen in [3] geven aan dat aan de eerste vereiste is voldaan. Aan de tweede eis wordt `a fortiori' voldaan omdat de pseudonimisering faciliteit zelf alleen publieke versleutelde BSN-hashes ontvangt die deze niet kan relateren. Vergelijk de laatste van bovengenoemde claims. Hiermee hebben we gemotiveerd dat zelfstandige pseudoniemen in het voorgestelde stelsel juridisch gezien geen persoonsgegevens zijn.

Implementatie van polymorfe pseudonimisering

Binnen de opzet beschreven in de introductie (punt 2) regelt de school de toegangsbeveiliging van de leerling tot de

Bij succesvolle authenticatie wordt deze identiteit door de school, via de browser van de leerling, naar de uitgever gestuurd

uitgeveromgeving. Deze opzet heet ook wel federatief. Binnen een dergelijke opzet wordt vaak de Security Assertion Markup Language (SAML) standaard toegepast. Deze standaard, zie [11], specificeert zowel de berichten tussen de leerling, school en uitgever maar ook de uitwisselingprotocollen daarvan. Binnen een standaard SAML-implementatie delen de school en uitgever een statische leerlingidentiteit. Bij succesvolle authenticatie wordt deze identiteit door de school, via de browser van de leerling, naar de uitgever gestuurd. Als de polymorfe opzet wordt toegepast om de leerlingprivacy te beschermen dan dient de school een gerandomiseerd encrypted pseudoniem naar de uitgever sturen in plaats van een statische identiteit. De uitgever moet dit vervolgens ontsleutelen tot het pseudoniem. Deze opzet is niet standaard binnen SAML en betekent dat de school pre-processing (de randomisering) en de uitgever post-processing (de ontsleuteling) moet doen. Bij de introductie van polymorfe pseudonimisering in 2014 binnen het eID2.0-ontwerp werd door ICT-leveranciers het bezwaar opgeworpen dat dergelijke pre- en post-processing mogelijk lastig zijn te implementeren binnen bestaande SAML-implementaties.
Onder meer naar dit aspect voert Hans Harmannij vanuit de Radboud universiteit zijn masters afstudeeronderzoek uit bij Surfnet. Hoewel zijn onderzoek nog niet is afgerond, is wel reeds gedemonstreerd dat bovenstaande opzet eenvoudig (binnen twee weken) kon worden geïmplementeerd in een gangbare SAML-implementatie. Het betrof daarbij een implementatie waarbij Microsoft's ADFS (Active Directory Federated Services) bij de school en SimpleSAMLPHP of Shibboleth bij een uitgever wordt gebruikt. Door de ontwikkelde software als open source beschikbaar te stellen zouden toekomstige implementaties van de polymorfe opzet verder kunnen worden vereenvoudigd. De polymorfe opzet lijkt aldus eenvoudig toepasbaar in combinatie met SAML.

Uitbreidingen

In deze sectie zullen wij beknopt de twee uitbreidingen uit [3] bespreken op de beschreven polymorfe infrastructuur: attribuutdiensten en een centrale inzagedienst.

Attribuutdiensten

Via een attribuutdienst kunnen met toestemming van de leerling/ouders persoonlijke gegevens ('attributen') worden verstrekt aan een uitgever. Typische voorbeelden van attributen zijn geboortedatum, geboorteplaats, adres. In veel gevallen zal de school zelf in staat zijn om attributen te verstrekken aan de deelnemers, maar in sommige gevallen zal hiervoor een derde partij (de attribuutdienst) ingezet kunnen worden. Hierbij zijn verschillende varianten mogelijk binnen de polymorfe opzet. In de basisvariant beschikt de attribuutdienst ook over eigen pseudoniemen van leerlingen en zijn deze verbonden met leerlingattributen. Als een uitgever over een dergelijk attribuut wil beschikken dan stuurt de uitgever daarvoor een attribuutverzoek naar de school samen met het encrypted pseudoniem van de leerling bij de school. De school herleidt hieruit het pseudoniem van de leerling. Als de school bepaalt dat aan dit verzoek gehoor kan worden gegeven dan stuurt de school een getekend toestemmingbericht naar de uitgever voor het opvragen van het attribuut. Daarin voegt de school zowel het encrypted leerlingpseudoniem bij de attribuutdienst als dat bij de uitgever toe. De uitgever stuurt dit toestemmingbericht naar de attribuutdienst. Deze laatste bepaalt het pseudoniem van de leerling en stuurt de gevraagde attributen naar de uitgever vergezelt van het encrypted leerlingpseudoniem bij de uitgever. De uitgever herleidt het leerlingpseudoniem en koppelt het attribuut daarmee.
Vaak maken gecombineerde attributen, zoals geboortedatum met postcode, het mogelijk om een persoon indirect mee te identificeren. Dit zorgpunt correspondeert overigens met de derde pseudonimiseringeis van de Autoriteit Persoonsgegevens in [10]. Om dit zorgpunt te adresseren wordt in [3] ook het concept polymorfe encryptie ontworpen. Hierbij beschikt de attribuut dienst alleen over versleutelde attributen die hij zelf niet kan lezen maar alleen kan omzetten naar een vorm die leesbaar voor anderen is. Deze opzet is ook ElGamal gebaseerd en vergelijkbaar met de techniek waarmee polymorfe pseudoniemen (voor niemand leesbaar) worden omgezet naar encrypted pseudoniemen (alleen leesbaar voor de bedoelde partij). Met de inzet van polymorfe attributen

worden de beveiliging- en privacy ('hotspot') risico's bij een attribuutdienst gereduceerd. De combinatie van polymorfe encryptie en pseudonimisering (PEP) maakt ook interessante toepassingen in andere sectoren mogelijk, bijvoorbeeld in de zorg. Het idee is dan dat (medische) gegevens vanuit verschillende bronnen (zorgverleners, laboratoria, apotheken maar ook sportapparatuur of -APPs) via PEP beschermd in de cloud worden geplaatst. Onder controle van de patiënt, kunnen dan delen van deze gegevens in gekoppelde vorm beschikbaar worden gemaakt voor behandelaars van de patiënt (inclusief persoonsgegevens) maar ook voor onderzoekers (in gepseudonimiseerde vorm). Bij de Digital Security groep van de Radboud Universiteit wordt op dit moment gewerkt aan een implementatie van deze opzet. Een vergelijkbare toepassing is mogelijk in de justitiële keten en stelt daar in staat dat verschillende partijen (politie, officieren van justitie, advocaten, rechters, jeugdzorg, gevangenissen, reclassering) kunnen samenwerken rond een individu zonder gebruik van persoonsnummers.

Centrale inzagedienst

Vanuit het recht op inzage (Wet bescherming persoonsgegevens, artikel 35) is het relevant een leerling of zijn ouders inzage te kunnen geven in:

- de scholen die de leerling hebben geregistreerd in de polymorfe infrastructuur, i.e. die encrypted pseudoniemen hebben opgevraagd voor de leerling bij de Nummervoorziening;
- de uitgevers voor wie deze scholen encrypted pseudoniemen hebben aangevraagd;
- de attributen die zijn geleverd aan uitgevers door attribuutdiensten.

Een centrale inzagedienst kan bovenstaande behoefte eenvoudig invullen. Het idee is dat de Pseudonimisering Faciliteit bij elk verzoek vanuit een school om een polymorf leerlingpseudoniem om te zetten in een encrypted pseudoniem, ook een encrypted pseudoniem maakt voor de centrale inzagedienst. Dat wil zeggen dat ook de inzagedienst zijn eigen pseudoniemdomein heeft. De Pseudonimisering Faciliteit stuurt dit encrypted pseudoniem vervolgens naar de inzagedienst samen met de details van het schoolverzoek, e.g. naam school, tijd, opgegeven uitgevers. De leerling (en zijn ouders) kan dan via zijn school inloggen bij de inzagedienst, zoals ook aangelogd kan worden bij een uitgever. Daarbij kan de leerling zien welke scholen namens hem verzoeken hebben gedaan en voor welke uitgevers of attribuutdiensten.

Referenties

[1] PBLQ HEC, Privacy Impact Assessment Nummervoorziening in de Leermiddelenketen, versie 1.0, 27 mei 2015. Zie https://www.rijksoverheid.nl/.

[2] HET EUROPEES PARLEMENT EN DE RAAD, Voorstel voor algemene verordening gegevensbescherming, 2012, COM/2012/011. Zie http://eur-lex.europa.eu.

[3] Eric Verheul, Privacy protection in electronic education based on polymorphic pseudonymization, 2015. Zie http://eprint.iacr.org/2015/1228

[4] Programma eID, Polymorphic Pseudonymization, versie 0.91, 7 juli 2014. Zie http://www.cs.ru.nl/E.Verheul/papers/eID2.0/PP_Scheme_091.pdf

[5] Zie http://www.pvib.nl/agendapunt/17701078/10-02-2015/Cryptonacht.

[6] Washington Post, Hacks of OPM databases compromised 22.1 million people, federal authorities say, 9 juli 2015. Zie http://www.washingtonpost.com.

[7] KrebsonSecurity, Online Cheating Site AshleyMadison Hacked , 19 juli 2015. Zie http://krebsonsecurity.com.

[8] T. ElGamal, A Public Key Cryptosystem and a Signature scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory 31(4), 1985, pp. 469-472.

[9] Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, CRC PRESS, 2008.

[10] Autoriteit Persoonsgegevens, Pseudonimisering risicoverevening, 6 Maart 2007. Referentie: z2006-1382.

[11] OASIS, Security Assertion Markup Language, versie 2.0. Zie https://wiki.oasis-open.org.

Mr. Rachel Marbus
@rachelmarbus op Twitter

PRIVACYVRIENDELIJKE BIG DATA: DAT KAN WÉL

Werken met veel gegevens is niet zo heel erg nieuw. Wat je daar allemaal mee kunt doen en de dingen die je eruit kunt halen als je daar slimme analyses op loslaat, is wel iets wat de laatste jaren een grote ontwikkeling heeft doorgemaakt. Er is daarbij gelukkig ook steeds meer aandacht en zorg voor het effect dat al die slimme analyses kan hebben op mensen. En dan met name de impact op privacy. Terecht worden vragen gesteld of dat wel allemaal zomaar kan. Al die slimme analyses brengen zaken boven waarvan we voorheen het bestaan niet wisten, nieuwe verbanden worden gelegd en nieuwe gegevens vloeien bijna als vanzelf voort uit de Big Data.

Je kunt vreselijk mooie innovatieve ontwikkelingen bedenken waarbij je gebruik maakt van die berg gegevens die tot je beschikking staat. En in een heel aantal gevallen is daarbij zelfs helemaal geen impact op privacy. Zo weten we bij NS door analyses van gebruiksgegevens dat een incheckpaaltje na een bepaald aantal malen "aangetikt" te worden, kapot gaat. De systemen zijn daardoor zo ingericht dat een tijd voordat dat kantelpunt bereikt wordt er automatisch een monteur naar het paaltje gestuurd wordt voor een onderhoudsbeurt. Ook dat is Big Data met slimme analyses. Reizigers en NS varen beide wel bij goed werkende paaltjes.

De zorg zit hem natuurlijk in die gevallen dat je wel met gegevens van personen gaat werken om slimme analyses te verrichten. En dan nog steeds is er binnen de wettelijke kaders heel veel mogelijk. Zo worden er binnen NS Extra analyses verricht op de check-in- en check-out-gegevens van personen om te bepalen waar iemand een check-out zou hebben gedaan indien hij dat vergeten is. Voordat reizigers zich opgeven voor NS Extra wordt hen verteld wat we met de gegevens doen en moeten ze daar expliciet toestemming voor geven. Meedoen hoeft niet, de oude procedures werken nog steeds en iedereen kan zijn geld terugkrijgen bij een vergeten check-out. De slimme analyse binnen NS Extra maakt het alleen veel makkelijker en sneller voor de reiziger. Dit zijn het soort cases waar het mes aan twee kanten snijdt. Begin klein en privacyvriendelijk met voordelen aan beide zijden van de medaille. Zorg er ook voor dat personen die niet mee willen doen, nog steeds van jouw diensten gebruik kunnen maken. Persoonsgegevens verwerken en daarop slimme analyses verrichten kan prima. Wees gewoon open, eerlijk, transparant en slim.

Kun je dan werkelijk alles doen met data als je maar toestemming hebt van klanten? Nee, natuurlijk niet. Uiteraard kan je met diezelfde bak gegevens heel veel privacyschendende analyses doen, maar dat is nu precies waarvan je weg moet blijven. En op dat snijvlak waar het begint te hellen en af te glijden, ligt een verantwoordelijkheid voor bedrijven en organisaties om heel dapper NEE te zeggen. Ook dat hoort bij privacy, bepalen waar de grens ligt en vaststellen wat de privacynormen en waarden zijn. Hoe wil jij bekend staan? Wat is de privacyreputatie die jij kan en wil verdedigen?

MELDPLICHT CYBERSECURITY VOOR EEN VEILIGER SAMENLEVING?

Terwijl in Brussel druk wordt onderhandeld over een nieuwe richtlijn informatiebeveiliging, heeft staatssecretaris Klaas Dijkhoff van Veiligheid en Justitie recent de 'Wet gegevensverwerking en meldplicht cybersecurity' naar de Kamer gestuurd. In deze blog een juridische en technische duiding van dit wetsvoorstel, aangevuld met enkele adviezen over dit belangrijke maatschappelijke thema.

Het wetsvoorstel introduceert een meldplicht voor vitale aanbieders wanneer een ICT-inbreuk kan leiden tot maatschappelijke ontwrichting. De melding moet worden gedaan bij het Nationaal Cyber Security Centrum (NCSC) en is tweeledig: enerzijds kan er door de melding een inschatting worden gemaakt van de maatschappelijke impact, anderzijds kan het NCSC aan de betreffende organisatie deskundige hulp en ondersteuning bieden.

Vitale aanbieders

De meldplicht geldt voor 'vitale aanbieders', zowel private als publieke organisaties. De staatssecretaris komt nog met een aanwijzing voor welke sectoren de meldplicht specifiek gaat gelden, maar hij heeft al toegezegd dat de meldplicht in ieder geval geldt voor de sectoren elektriciteit, gas, drinkwater, telecom, financiën, overheid, transport (mainports Rotterdam en Schiphol) en nucleair.

Wanneer melden?

Als er sprake is van een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit (in het wetsvoorstel worden overigens de informatiebeveiligingstermen 'beschikbaarheid', 'integriteit' en 'vertrouwelijkheid', naast het begrip 'betrouwbaarheid' niet consequent gebruikt) van een elektronisch informatiesysteem moet er worden gemeld. Opvallend is dat er geen melding van een DDoS-aanval hoeft te worden gedaan, omdat dit slechts een verstoring betreft. Opmerkelijk, want bij vitale procesbesturing kan een DDoS-aanval echter wel tot ernstige problemen leiden, denk aan bruggen die niet open of dicht gaan omdat het internetkoppelvlak overbelast is.

Rol NCSC

De meldplicht is primair gericht op het bieden van hulp, waarbij het NCSC fungeert als een informatieknooppunt voor informatie en advies. De staatssecretaris is verstandig geweest door in het wetsvoorstel op te nemen dat gevoelige, door de aanbieders verstrekte informatie aan het NCSC, niet 'WOB-able' is.
Het NCSC is niet bevoegd om dadergericht onderzoek te doen en mag geen interventies plegen. De informatie- en adviesfunctie lijkt hierdoor beperkt. Daar komt bij dat er voor de naleving van de meldplicht geen toezicht en sancties gelden. Naar verwachting zal de aankomende Europese richtlijn informatiebeveiliging deze verplichting wel bevatten.

Hoe nu verder?

De staatssecretaris wil, analoog aan de luchtvaartsector, een just culture creëren waarbij gezamenlijk wordt bijgedragen aan veiligheid. Daar past een terughoudende rol van het NCSC bij. De toekomst zal uitwijzen of vitale organisaties zich in deze cultuur herkennen of dat toch verlangt wordt naar een sterkere positie voor het NCSC (of een toezichthouder) met passende bevoegdheden.

ing. Renato Kuiper CISSP CISA en is management consultant bij Verdonck, Klooster & Associates. Renato is te bereiken via renato.kuiper@vka.nl.
mr. Bas de Groot en is consultant bij Verdonck, Klooster & Associates. Bas is te bereiken via bas.degroot@vka.nl.

eIDAS VERORDENING

Een Europees kader voor betrouwbaarheidsniveaus van online diensten

Per 1 juli dit jaar wordt de Europese eIDAS-verordening van kracht [1]. Deze verordening leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. Dit heeft gevolgen voor online overheidsdiensten. Het heeft ook gevolgen voor DigiD, eHerkenning, het Idensys-stelsel en PKIoverheid. Dit artikel legt uit wat de verordening over betrouwbaarheidsniveaus zegt. Samengevat gaat het om een niveau laag dat ruwweg overeenkomt met DigiD Basis, een niveau substantieel dat vergelijkbaar is met de meeste middelen voor internetbankieren en een niveau hoog dat in de Nederlandse praktijk door PKIoverheid wordt ingevuld. Naast betrouwbaarheidsniveaus biedt de eIDAS-verordening een vernieuwd stelsel voor elektronische handtekeningen. Deze zijn in de bredere context van "vertrouwensdiensten" gezet.

Wat verstaan we onder een betrouwbaarheidsniveau? Betrouwbaarheidsniveaus hebben betrekking op authenticatiemiddelen en elektronische diensten. De risico's die een bepaalde online dienst met zich meebrengt, bepalen welke maatregelen genomen moeten worden. De middelen waarmee gebruikers zich bij de dienst bekend maken, zijn een belangrijk aspect daarvan. Voor de ene dienst volstaat een social login, voor een andere dienst is het aanbieden van een specifieke smartcard vereist. Bovendien worden deze authenticatiemiddelen in toenemende mate voor zoveel mogelijk verschillende diensten gebruikt. Dat geldt voor social logins zoals Facebook of Google, maar het geldt ook voor DigiD. Wanneer je een type middelbreed wilt gebruiken, is het belang van betrouwbaarheidsniveaus groter. Je moet dan immers een manier hebben om te bepalen welke groepen van middelen geschikt zijn voor welke diensten. Tot op heden hanteerden we hiervoor de in het Europese STORK-programma

Michael Stoelinga werkt voor Capgemini als business architect publieke sector. Hij is gespecialiseerd in basisregistraties en identiteitsmanagement. Afgelopen jaren droeg hij bij aan opdrachten voor eHerkenning, DigiD en identity management binnen uitvoeringsorganisaties. Hij is lid van de klankbordgroep "handreiking classificatie betrouwbaarheidsniveaus" van het Forum Standaardisatie. Hij is bereikbaar via michael.stoelinga@capgemini.com. https://nl.linkedin.com/in/mstoelinga

Figuur 1 - Twee kanten van de betrouwbaarheidsniveaus.

opgestelde criteria. Deze zijn toegepast in eHerkenning en in het ontwerp voor Idensys. Met Idensys wordt het stelsel bedoeld dat de volgende generatie van DigiD en eHerkenning gaat vormen. Dit wordt momenteel ontwikkeld in de vorm van pilots. Diverse belangrijke keuzes over de invulling ervan moeten dit jaar genomen worden. Zie Vervolgbrief pilots eID van 15 december 2015 [2].

Om overheidsdienstverleners te ondersteunen met het inschalen van hun diensten is door het Forum Standaardisatie de Handreiking Betrouwbaarheidsniveaus opgesteld [3]. In het kader van eIDAS zal deze handreiking worden bijgewerkt.

Figuur 1 geeft de twee kanten van betrouwbaarheidsniveaus weer. Links staat de vragende kant: de eis die gesteld wordt om een elektronische dienst te mogen gebruiken. Rechts staat de aanbiedende kant: het niveau dat door een bepaald authenticatiemiddel geboden wordt.

Context van de eIDAS-verordening

eIDAS is een Europese verordening. Dat betekent dat het vanaf de ingangsdatum ook in Nederland geldt als wet. Bestaande Nederlandse wetgeving wordt erdoor vervangen, evenals de eerdere Europese richtlijn over elektronische handtekeningen. De keuze om een verordening op te stellen, is een duidelijk geval van Europees beleid. Beleid gericht op een sterke positie van Europa in de digitale wereld. Een soortgelijke verzwaring wordt in komende jaren doorgevoerd voor de privacywetgeving (General Data Protection Regulation [4]).

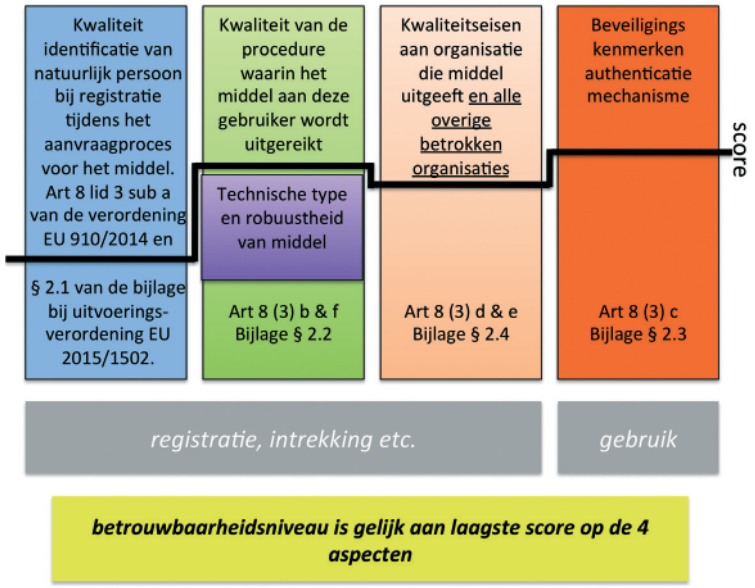
Zoals veel Europese instrumenten komt dit beleid tot stand via regels over grensoverschrijdend verkeer. Voor online dienstverlening van de overheid wordt geregeld hoe deze toegankelijk moeten zijn vanuit andere Europese landen. Dit werkt vervolgens door in het eigen land. En dat is precies wat het Europese beleid beoogt. Het is een volgende stap op weg naar grotere standaardisatie van eID's. De ervaring met de eerdere wet- en regelgeving is dat deze standaardisatie minder snel gaat dan sommigen hoopten. Dit wordt gezien als een van de grootste hobbels om alle overheidsdiensten voor eind volgend jaar digitaal aan te bieden, ofwel "Digitaal 2017" zoals dat in de beleidsstukken heet (zie [2]).

De eIDAS-verordening staat uiteraard ook in de context van de toenemende aandacht voor digitale fraude en de discussies over privacy. Deze ontwikkelingen vragen om eID's met een hoger betrouwbaarheidsniveau.

Drie betrouwbaarheidsniveaus

In de verordening worden drie betrouwbaarheidsniveaus gedefinieerd: laag, substantieel en hoog. Deze zijn uitgewerkt in een uitvoeringsverordening [5]. Op hoofdlijn komen deze overeen met de eerder in het STORK gedefinieerde niveaus twee tot en met vier [6]. De opbouw van de eisen per niveau is vergelijkbaar. In vergelijking met STORK en ISO 29115 is de tekst van de uitvoeringsverordening abstracter. De formulering geeft het resultaat aan dat met een bepaalde controle bereikt moet worden. Er wordt niet gespecificeerd hoe dat moet worden ingevuld. STORK en ISO 29115 worden wel uitdrukkelijk genoemd. Waar die bronnen meer specificaties geven voor het "hoe" kunnen ze dus niet worden genegeerd.

Figuur 2 geeft een overzicht van de aspecten waarop het



Figuur 2 - Beoordelingsaspecten van het betrouwbaarheidsniveau.

betrouwbaarheidsniveau beoordeeld wordt met verwijzingen naar de uitvoeringsverordening. De zwarte lijn geeft de score weer van een bepaald betrouwbaarheidsmiddel. Bepalend is daarbij uiteraard de zwakste schakel. De opbouw is analoog aan de weergave van de STORK-eisen in de handreiking betrouwbaarheidsniveaus van Forum Standaardisatie [3].

Het betreft de volgende aspecten:

- Aanvraagproces, identiteitsverificatie en registratie
- Type middel inclusief uitgifte- en verlengingsproces
- Eisen aan de organisaties die in aanvraag, uitgifte en gebruik betrokken zijn
- Authenticatiemechanisme (technisch), ieder keer dat het middel gebruikt wordt

Het laagste STORK-niveau is in eIDAS buiten beschouwing gelaten. Dat niveau geeft geen zekerheid dat het authenticatiemiddel door één en dezelfde persoon gebruikt wordt. Het betreft bijvoorbeeld aanmelding bij een website op basis van e-mailverificatie of een eenvoudige social login.

Niveau laag

Dit niveau is dus vergelijkbaar met STORK 2, het niveau dat we in Nederland kennen van DigiD Basis. Globaal zijn de eisen dat bij aanvraag identiteitsgegevens worden opgegeven die uniek genoeg zijn en overeenkomen met de naam die betreffende persoon in zijn paspoort heeft staan. Let wel, er mag aangenomen worden dat de gegevens overeenkomen. Het paspoort of een ander wettelijk identificatiedocument (WID) hoeft niet gecontroleerd te worden. Het hoeft ook niet zeker te zijn dat de persoon daadwerkelijk de WID in bezit heeft. Ten tweede moeten de gegevens gecontroleerd worden in een authentieke bron. Dit kan een controle in de Basisregistratie Personen zijn. Het mag ook een daarvan afgeleide controle zijn. Van gegevens van een persoonlijke bankrekening, mobieletelefoonabonnement of een personeelsdossier bij de werkgever kan in Nederland verwacht worden dat deze zijn terug te voeren op een WID. Een single-factor-middel volstaat. De beveiligingscontroles moeten bescherming bieden tegen Common Criteria enhanced-basic aanvalspotentieel. In de Nederlandse versie van de uitvoeringsverordening is dit overigens ten onrechte met "laag" vertaald, zie ISO/IEC 18045:2008 bijlage B [7], waar het 'basic' heet.

Niveau substantieel

Bovenop niveau laag vereist dit een twee-factor-middel. Dat is uiteraard voor gebruikers een duidelijk merkbaar verschil. Substantieel eist dit niveau echter heel wat meer dan enkel het sterkere middel. In het aanvraagproces wordt een of andere vorm van controle van een identiteitsdocument vereist. De uitvoeringsrichtlijn geeft aan dat tonen van een identiteitsdocument een mogelijkheid is, maar geeft ook de optie van een verificatie op een andere manier. Verificatie door de werkgever of toepassen van Remote Document Authenticatie (RDA)-technologie[8] valt daaronder. De aanbieder van het middel moet verdere controles uitvoeren, waaronder de BKR-VIS-toetsing op vermiste of gestolen WIDs.

Het gaat echter niet alleen om het aanvraagproces. Het twee-factor middel moet ook "zodanig ontworpen zijn dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon te vallen aan wie het toebehoort." Dat betekent dat het opsturen van een kopie of scan van paspoort als

optie vervalt. Het is te gemakkelijk om zo'n kopie te maken zonder dat de eigenaar er toestemming voor heeft gegeven. Ook is het niet zeker dat de verzwaring van DigiD met RDA-technologie zonder meer leidt tot "substantieel". Alleen als iedereen die een rijbewijs met NFC-chip heeft deze in een metalen hoesje houdt, wordt echt aan de eis voldaan. De recente commotie over uitlezen van contactloze bankpassen laat zien dat we dat niet zomaar weg kunnen poetsen.

Ook over het sturen van een code per SMS naar de telefoon is discussie mogelijk. Veel mensen hebben hun telefoon altijd in hun zak (of in de hand), dan zal het niet makkelijk zijn een code af te kijken. Maar hoe vaak zien we een slingerende telefoon? Wie denkt eraan als zijn telefoon is gestolen, dat het gebruik ervan als tweede factor vervalt. Tenslotte is de vraag of een smartphone een echte tweede factor is. Als het wachtwoord als eerste factor op hetzelfde toestel wordt gebruikt is er een fors risico. Die situatie voldoet eigenlijk niet meer aan de vereiste bescherming tegen aanvallers met een "gematigd" aanvalspotentieel. Ook hier zijn de Common Criteria relevant. Voor substantieel moet bescherming geboden worden tegen een "moderate" aanvalspotentieel. Expliciete toestemming van de gebruiker voor iedere keer inloggen is daarvoor een eis. In de uitvoeringsverordening staat tenslotte nog de eis van "dynamische authenticatie". Dit stelt eisen aan de protocollen waarmee de authenticatie wordt uitgevoerd. Allemaal zaken die het onterecht gebruik van het middel flink moeilijker moeten maken dan op niveau laag.

Tenslotte stelt niveau substantieel hogere eisen aan de informatiebeveiliging van betrokken organisaties. Dit moet aan beproefde normen voldoen en onafhankelijk geaudit worden.

Uit deze eisen valt te concluderen dat de lat voor de nu lopende pilots van Idensys en andere projecten om DigiD een hoger betrouwbaarheidsniveau te geven hoger ligt dan enkel een twee-factor-middel aanbieden. Met name de details van het aanvraagproces en de zekerheid dat de gebruiker bewust zijn "tweede factor" gebruikt, zijn daarbij bepalend.

Niveau hoog

Wat niveau hoog betreft is het belangrijkste dat dit in eIDAS niet gelijk gesteld wordt met het niveau van de gekwalificeerde elektronische handtekening. Dit was bij STORK 4 overigens ook niet het geval. De gekwalificeerde elektronische handtekening valt in eIDAS onder de vertrouwensdiensten en wordt los van de betrouwbaarheidsniveaus voor eIDs beschreven. Voor eIDAS niveau hoog moeten er in ieder geval fysieke kenmerken gecontroleerd worden. Dit vereist een vorm van face-to-face-contact. Een foto volstaat maar controle van een ander biometrisch kenmerk mag ook. De formulering is minder expliciet dan bij Stork. Het verifiëren van biometrische kenmerken op afstand – indien daar in de toekomst een methode voor ontstaat die goed genoeg is – wordt mijns inziens niet uitgesloten. Een voorbeeld van dergelijke methodes is de door de Duitse financieel toezichthouder ontwikkelde controle via een videoverbinding [9].

Vreemd genoeg is deze zwakkere formulering via artikel 24 sub 1b ook van toepassing op gekwalificeerde vertrouwensdiensten. Dat lijkt, zoals al eerder opgemerkt in de reactie van de iTrust Foundation in de openbare consultatie over eIDAS, een vergissing van de Europese regelgever [10]. Wat betreft het middel zelf zijn de eisen voor hoog gekoppeld aan Common Criteria high attack potential. Dat betekent dat alle denkbare maatregelen tegen man-in-the-middle-/man-in-the-front-aanvallen ingebouwd moeten worden. Dit heeft ook tot gevolg dat Single Sign-on over meerdere diensten heen ongewenst is. De gebruiker moet expliciet betrokken zijn in het toegang krijgen tot iedere dienst afzonderlijk.

Het grote verschil tussen niveau hoog en gekwalificeerde vertrouwensdiensten zit in de aansprakelijkheid. Voor gekwalificeerde vertrouwensdiensten geldt een "omgekeerde bewijslast" (art. 13). Dat is niet gewijzigd ten opzichte van de huidige wetgeving. Dit betekent dat bij een vermeende inbreuk wordt aangenomen dat de vertrouwensdienst aansprakelijk is, tenzij deze kan aantonen dat aan alle regels – zoals de precieze identiteitsverificatie – is voldaan. Dit leidt in het algemeen tot het precies vastleggen van processen door de aanbieder.

Het effect van "open grenzen"

Artikel 6 van de verordening gaat over het erkennen van authenticatiemiddelen van andere EU-landen. Het artikel maakt een belangrijk verschil tussen niveau laag en de niveaus substantieel en hoog. Wanneer een overheidsdienst wordt aangeboden op niveau substantieel of hoog, dan is het vereist dat deze ook toegankelijk is met middelen uit andere EU-landen. Dat geldt dan uiteraard alleen voor middelen die in dat land tenminste ook substantieel of hoog zijn. Voor niveau laag is deze grensoverschrijdende werking niet verplicht. Praktisch zal deze toegang verlopen via een koppelpunt dat de overheid inricht. Dit koppelpunt zal aangesloten worden op het Idensys-stelsel.

De consequentie is dat een Nederlandse overheidsdienst die diensten op een hoger betrouwbaarheidsniveau gaat aanbieden gedwongen wordt om deze ook open te stellen voor buitenlandse middelen. Deze consequentie gaat pas gelden wanneer Nederland Idensys of één van de andere

stelsels aan middelen aanmeldt om mee te draaien in dit Europese stelsel. Zonder een dergelijke aanmelding kunnen Nederlanders echter ook geen toegang krijgen in die andere landen. De aanmelding is dan ook gepland voor het Idensys-stelsel. Dit kan bijvoorbeeld betekenen dat de Belastingdienst het berichtenverkeer voor omzetbelasting moet openstellen. Daar wordt nu immers een PKIo-certificaat vereist waarvan je kunt stellen dat het overeenkomt met niveau hoog. Dit vereist dan dat zo'n precies dienst conform de standaarden gaat werken. Het is afwachten hoe de Nederlandse overheid hiermee om zal gaan.

Effecten van de verordening

Het duidelijke wettelijk kader dat hiermee tot stand komt zal overheden helpen om elektronische diensten op een consistent betrouwbaarheidsniveau te realiseren. De snelheid waarmee dit gebeurt zal afhangen van de beslissingen die genomen moeten worden over Idensys. Op dit moment lopen er meerdere pilots. Op verschillende manieren wordt geprobeerd om een betere versie van DigiD te realiseren. Het doel is het grote volume en brede gebruik van DigiD vast te houden, maar dan op niveau substantieel. De politiek heeft zich uitgesproken voor een multi-middelenstrategie. Daardoor zal er een stelsel ontstaan waarin verschillende middelen gebruikt kunnen worden. Dit sluit goed aan op de eIDAS-verordening. Als het meezit kunnen beide ontwikkelingen elkaar versterken. De ruimte voor een overheidsdienst om eigen oplossingen te kiezen wordt in ieder geval kleiner. Als het tegenzit stroomt er eerst nog flink wat water door polderland voordat een echte richting wordt gekozen. In dat geval vormt de toegang vanuit het buitenland een stok achter de deur. Hoe dan ook gaan daar dan de invoeringstermijnen van deze verordening over heen.

Voor de private sector zijn er geen directe gevolgen. Naarmate het volume van online overheidsdiensten groeit, kunnen de eisen die daaraan gesteld worden invloed hebben op de markt. Mocht het zo zijn dat in het kader van Idensys een stelsel tot stand komt met zowel publieke als private middelen dan zal de koppeling directer worden. In een dergelijk stelsel zijn er middelen die zowel voor overheidsdiensten als voor bijvoorbeeld internetbankieren gebruikt worden. De vraag of alle internetbankiermiddelen aan niveau substantieel voldoen, wordt dan sneller gesteld.

Conclusie: een bruikbaar kader

De verordening leidt tot een bruikbaar kader. Betrouwbaarheidsniveaus zijn belangrijk genoeg voor deze wettelijke basis. De formulering sluit aan op standaarden als ISO 20115 en STORK die de afgelopen jaren al hun bijdrage hebben geleverd. Doordat betrouwbaarheidsniveaus onderdeel zijn geworden van de bredere eIDAS-verordening zal de toepassing en standaardisatie sneller gaan. Op enkele punten is de uitvoeringsverordening duidelijker, maar ten aanzien van de face-to-face-controle voor gekwalificeerde certificaten kan er een nieuwe onduidelijkheid ontstaan. Voor de toepassing in Nederland is het van belang dat de nieuwe verordening wordt omgezet in praktische normenkaders en dat praktijkervaringen gedeeld worden.

Referenties

[1] Verordening (EU) Nr. 910/2014 – 23 juli 2014 http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910

[2] Vervolgbrief pilots eID van 15 december 2015 nummer 26643-379 http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z24493&did=2015D49561

[3] Handreiking Forum Standaardisatie. Betrouwbaarheidsniveaus voor elektronische overheidsdiensten (versie 3) https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_v3__2014_.pdf

[4] Stand van zaken EU verordening over bescherming persoonsgegevens GDPR https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/07/tk-eu-pakket-bescherming-persoonsgegevens.

[5] Uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen. http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015R1502&from=NL

[6] STORK. Secure idenTities acrOss boRders linKed. Zie document D2.3 ? Quality authenticator scheme,paragraaf 2.3 en 2.4, te vinden op www.eid?stork.eu, onder STORK materials, deliverables approved/public.

[7] ISO/IEC 18045:2008 - Information technology -- Security techniques -- Methodology for IT security evaluation: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46412

[8] RDA: https://www.rijksoverheid.nl/documenten/formulieren/2015/12/10/digid-proef-met-remote-document-authentication en https://www.youtube.com/watch?v=AwiASv9cz50&feature=youtu.be

[9] BAFIN (Bundesanstalt fu?r Finanzdienstleistungsaufsicht (Bafin, Interpretation of section 6 (2) no. 2 of the GwG ("not personally present"), 2014. http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm_en.html?nn=2821306#doc5295362bodyText3

[10] https://www.itrust.foundation/nieuws/standpunt-platform-trust-services-over-uitvoeringswet-elektronische-identificatie-en-vertrouwensdiensten-aan-ministerie-van-ez-gestuurd

MELDPLICHT DATALEKKEN

Wat wordt er van organisaties verwacht? (deel 2)

In twee publicaties in het vakblad van PvIB bespreken wij een lijst van negen maatregelen voor passende beveiliging van persoonsgegevens. In deel 1 bespraken we maatregel 1 tot en met 5. Deze hadden betrekking op: het beleidskader, assessments, bewerkersovereenkomsten, gebruikersbewustzijn en toegangscontrole. In deze uitgave worden maatregel 6 tot en met 9 besproken.

6. Security Monitoring

Onder deze noemer verstaan wij twee elementen die de Autoriteit Persoonsgegevens los noemt.

Beheer van technische kwetsbaarheden

Dit proces (waar vaak de Engelse term "Vulnerability Management" voor wordt gebruikt) start met een "asset scan" om in kaart te brengen welke onderdelen aanwezig zijn in het netwerk en hier een waarde aan te geven. Via vulnerability-scans en audits wordt duidelijk of de betreffende assets voldoen aan het beleid of eventueel kwetsbaarheden bevatten die gevoelige informatie bloot zouden kunnen leggen.
Door de waarde van de assets te koppelen aan de gevonden kwetsbaarheden kan een risico worden opgesteld en kunnen acties worden uitgezet om de systemen op het juiste beveiligingsniveau te brengen.

Logging & controle

De Autoriteit verwacht dat activiteiten die gebruikers uitvoeren met persoonsgegevens, worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens, en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logging moet periodiek en actief worden gecontroleerd op verdacht gedrag en bij afwijkingen moet actie worden ondernomen. Concrete maatregelen zijn in de volgende drie categorieën op te delen.

1) **Genereren van logs.** Om tot een passend detailniveau binnen logs te komen, is het raadzaam om netwerkverkeer volledig te inspecteren, alsmede gedragingen binnen computersystemen. Hiervoor kunnen Intrusion Detection Systemen (IDS) of de nieuwste generatie firewalls (NGFW) worden gebruikt. Voor monitoring binnen computersystemen is ook Intrusion Detection-technologie voorhanden.
De Autoriteit wijst er wel op dat dit soort inspectie wellicht valt onder het instemmingsrecht van de ondernemingsraad, volgens artikel 27 van de Wet op de Ondernemingsraden (WOR). De gegenereerde logs bevatten immers waarschijnlijk informatie die herleidbaar is tot personen en er is dus sprake van een "personeelsvolgsysteem".

2) **Opslaan van logs.** Het is belangrijk om de logs centraal te verzamelen. De Autoriteit gaat uit van een minimale bewaartermijn van 1 jaar. Om de omvang van de dataopslag te beperken, is het verstandig om filtering en aggregatie toe te passen. Dit is mogelijk met Security Information & Event Management-technologie (SIEM).

3) **Beheren van logs.** De bovengenoemde tools zijn nodig, maar maken het verhaal nog niet compleet. Het is voor de eis van periodieke controle belangrijk operationeel securitybeheer uit te voeren. Daarbij is "periodiek" een ruim begrip. Het doel is om verdacht gedrag te herkennen en statistieken wijzen uit dat digitale inbraken vaak slechts in enkele uren uitgevoerd worden. Het is daarom raadzaam om de logs meerdere malen per dag te controleren. Afhankelijk van de organisatie eventueel ook buiten kantooruren.

7. Databescherming

Voor de bescherming van digitale persoonsgegevens noemt de Autoriteit in de richtlijnen de volgende specifieke maatregelen.

Validatie op gegevensbewerking

Hier wordt gedoeld op het controleren van invoer, interne verwerking en uitvoer van data in applicaties. Dit kan deels via de applicaties zelf, maar het kan voorkomen dat dit voor bepaalde werkzaamheden niet voldoende controle biedt. In die gevallen kunnen aanvullende maatregelen wenselijk zijn, zoals: "Data Loss Prevention (DLP)" en "File Integrity Monitoring (FIM)", d.w.z. het met software bewaken van integriteit in het bestandssysteem. Bij dit soort controles is het ook belangrijk om na te denken over mobiele apparatuur (laptops, maar eventueel ook tablets en smartphones) wanneer deze zich buiten het netwerk bevindt.

Versleuteling

De Autoriteit stelt dat sterke versleuteling de verplichting kan wegnemen dat naast de Autoriteit ook betrokkenen over het datalek moeten worden geïnformeerd. Zo kan dus ook voorkomen worden dat een incident in de publiciteit komt. Wel moet de versleuteling dan ook goed worden toegepast, in de zin dat zij toekomstbestendig is.

> Bij versleutelingswijzen die in een actuele beoordeling door ENISA worden gekwalificeerd als geschikt voor 'future use' (toekomstvast voor de komende 10 tot 50 jaar) kunt u ervan uitgaan dat de versleuteling sterk genoeg is.

De Autoriteit verwijst dus naar de beoordeling van de European Union Agency for Network and Information Security (ENISA) om te bepalen of de versleuteling "sterk" is [1].
Belangrijk is om bij versleuteling het verschil tussen data-at-rest (data die staat opgeslagen) en data-in-motion (data die wordt verzonden) in acht te nemen. Bij versleuteling van data-at-rest kan worden gedacht aan geïntegreerde versleuteling in databasestructuren of versleuteling op bestandsniveau. Voor data-in-motion is het met name van belang om na te denken over versleuteling van e-mail en van eventuele andere netwerkprotocollen zoals http.

Remote wiping

De Autoriteit verwijst ook expliciet naar "remote wiping" als effectieve maatregel om een verplichte melding aan betrokkenen te vermijden. Met remote wiping wordt bedoeld dat een computer op afstand de opdracht gegeven kan worden om data te vernietigen. Het kan wel lastig zijn om aan te tonen dat een remote wipe-actie ook inderdaad geslaagd is.

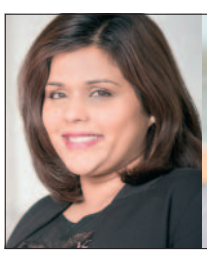
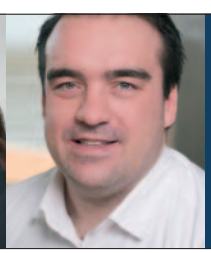
8. Incidentenbeheer

Zoals eerder gesteld, is het beheren van logs een belangrijke taak, omdat daarmee incidenten kunnen worden gesignaleerd. De Autoriteit vindt het belangrijk dat de opvolging van incidenten aantoonbaar goed geregeld is. Daarbij worden expliciet genoemd:

1. Risico-inschatting van het incident
2. Informeren van betrokkenen en toezichthouders
3. Geleerde lessen gebruiken voor aanscherping beveiliging
4. In geval van juridische vervolgstappen: verzameling van bewijsmateriaal

Ten aanzien van stap 2 vormen nu juist de meldplicht datalekken en de bijbehorende richtsnoeren een belangrijke ontwikkeling. De richtsnoeren geven in handige stroomdiagrammen aan of en hoe er in bepaalde gevallen gemeld moet worden. Daarbij geldt een aantal kernpunten:

- Er zijn twee soorten meldingen: de melding aan de Autoriteit en de melding aan betrokkene(n).
- Onder datalek verstaat men: "(...) de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan."
- De melding aan de Autoriteit:
    - moet gedaan worden als het datalek betrekking heeft op persoonsgegevens;
    - moet uiterlijk op de tweede werkdag na detecteren van het lek gedaan worden;
    - moet op die tweede werkdag alvast gedaan worden als nog niet met zekerheid is vastgesteld of een lek

Deze tekst is samengesteld door Nandenie Moenielal, Senior Security Consultant en Erik Remmelzwaal, Algemeen Directeur, beide werkzaam bij Nederlands security specialist DearBytes. Vragen of opmerkingen kunt u richten aan nandenie.moenielal@dearbytes.nl of via de website op dearbytes.com/wbp.

De Autoriteit benadrukt een aantal keer dat het niet voldoende is om te zeggen dat een bepaalde maatregel de schade heeft beperkt

persoonsgegevens betreft (omgekeerde bewijslast). Deze melding kan later eventueel worden ingetrokken;
  - moet vermelden of het lek al aan betrokkene(n) is gemeld en zo niet, wanneer dat gaat gebeuren.
- De melding aan betrokkene(n):
  - is niet nodig als beveiligingsmaatregelen voldoende bescherming bieden (denk aan versleuteling en remote wiping);
  - is daarna alleen nodig als het lek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkene.

9. Controle op naleving

Tot slot is controle op naleving een primair onderdeel van het privacyraamwerk. De Autoriteit benadrukt een aantal keer dat het niet voldoende is om te zeggen dat een bepaalde maatregel de schade heeft beperkt. De effectiviteit van de maatregel moet zodanig aangetoond worden, dat verlies en/of onrechtmatige verwerking van gegevens uitgesloten kan worden, en daarmee ook ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene, zodat een melding aan betrokkene achterwege gelaten kan worden.
Controle op naleving kan uitgesplitst worden naar verschillende niveaus:

- **Controle op werking van het privacyraamwerk:**
  Denk hierbij aan monitoring en naleving van het privacybeleid, het periodiek beoordelen van privacyrisico's en een goed functionerende rol van Functionaris Gegevensbescherming (FG). Dit kan vastgesteld worden door een interne audit uit te voeren. De Autoriteit verwijst naar de 'Privacy Audit Proof [2] als compliance-check. De Privacy Audit Proof is afkomstig van het NOREA en geeft de mogelijkheid voor een externe audit en certificering.

- **Controle op werking van getroffen maatregelen:**
  Middels interne controles en interne audit-assessments kan de effectiviteit van de maatregelen worden bepaald. Aansluitend op het voorbeeld van versleuteling kan regelmatig worden vastgesteld of aan de toetsingscriteria wordt voldaan.

- **Controle op werking van de PIA**
  Bij het uitvoeren van de PIA moet ook worden nagedacht door wie en op welke manier de acties gemonitord worden. In principe is de FG de aangewezen persoon hiervoor.

Zoals gezegd is controle op naleving (en eventuele bijsturing) de laatste stap in het privacyraamwerk (PDCA-concept). Er wordt door de Autoriteit geadviseerd om minimaal 1x per jaar te evalueren of de technische maatregelen passende bescherming bieden.

Conclusie

De verwachtingen die de Autoriteit Persoonsgegevens heeft bij de beveiliging van persoonsgegevens, zijn behoorlijk concreet. Ook al vormen ze geen wettelijke verplichting: toch is er, met de boetebevoegdheid in het achterhoofd, alle reden toe om zoveel mogelijk aan die verwachtingen te voldoen. Wie al vaker met het informatiebeveiligingsbijltje gehakt heeft, zal veel gelijkenissen herkennen met standaarden zoals ISO27000 en NEN7510. Een werkend Information Security Management Systeem (ISMS) zal waarschijnlijk maar op enkele punten moeten worden aangescherpt om de Autoriteit te overtuigen.
Maar voor organisaties die nog maar weinig hebben geregeld voor informatiebeveiliging, zal de hoeveelheid maatregelen best overdonderend overkomen. De kunst is dan om het geheel in kleinere, overzichtelijke stappen op te delen en dat kunnen prima de 9 stappen zijn, ook in die volgorde, zoals in deze 2 artikelen beschreven. De extra operationele taken zoals security-monitoring kunnen eventueel extern worden belegd door middel van outsourcing. Hoe dan ook gaat dat tijd en geld kosten en waarschijnlijk meer dan directies zich zouden beseffen.

Maar niets doen is ook geen optie. Want elke bestuurder van een organisatie waarop de privacywetgeving van toepassing is, zal het onderwerp 'privacy' hoog op de agenda hebben staan. Niet alleen om te voldoen aan wet- en regelgeving, maar ook vanuit een verantwoordelijkheidsgevoel dat past bij een internationaal mensenrecht. Grotere aandacht vanuit media, overheid, burgers, klanten, leveranciers en niet in de laatste plaats toezichthouders zal de organisatie stimuleren om zo snel mogelijk tot actie over te gaan. (auteurs worden weer in de koptekst benoemd)

Referenties

[1] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms- key-size-and-parameters-report-2014
[2] https://www.privacy-audit-proof.nl/

AAN ZEE GENIETEN VAN SECURITY

September vorig jaar vond de eerste editie van Security Summit @ The Beach plaats. Toen ik gebeld werd door de organisatie met de vraag of ik daar wilde spreken, hoefde ik niet heel erg lang na te denken. Ik ben geboren aan zee, bevind me graag op de golven, woon op een steenworp afstand van het stand: de zee zit in mijn bloed. En dan juist daar de gelegenheid te krijgen om te spreken over dat andere waar mijn hart sneller van gaat kloppen: privacy & security. Het was voor mij een match made in heaven.

Ikzelf sprak er over een flink privacy-incident waar ik als Privacy Officer van NS mee te maken heb gehad. Over de schrik die je om het hart slaat – ongelukken gebeuren overal, maar ze ontdekken is nog immer bijzonder onaangenaam – en hoe je dan vervolgens zo goed mogelijk het incident oplost en afhandelt. Met zeer veel plezier heb ik ook geluisterd naar Jaya Baloo, de CISO van KPN. Jaya verhaalde met een ongekende passie over "de" oorlog. Voor ons security-minnend volk betekent dat natuurlijk niet die van '40-'45 maar de weer opgelaaide oorlog over cryptografie. De belangrijkste boodschap die ze bij mij achterliet was dat het de hoogste tijd is dat wij op de barricades moeten om privacy en security uit te dragen, uit te leggen en er zo voor te zorgen dat op politiek niveau niet de verkeerde beslissingen worden genomen. De lezing van Jaya is via de site van het event terug te zien, het is zeer de moeite waard.

Dit jaar dan alweer de tweede editie. 30 juni 2016 weer een Security Summit @ The Beach. Twee sprekers zijn al bekend. Barry van Kampen, hacker extraordinaire, mede-oprichter van de hackerspace in Utrecht en onderdeel van het beruchte Hack in the box zal de summit openen. De afsluitende eer ligt bij Melanie Rieback, mede-oprichter van Radical Open Security, kick-ass wetenschapper en oprichter van de Dutch Girl Geek Dinner. Ik zal er in ieder geval bij zijn, dit jaar alleen als toehoorder, maar dat gaat met deze sprekers in ieder geval vast heerlijk worden.

Inschrijven kan via de website en wie snel is, kan tot en met 30 april nog de early bird korting meepikken. Eten en drank is inbegrepen bij de prijs en je kunt ook aan je verplichte punten komen. Na afloop krijg je per mail een certificaat van deelname aan het event. Dit kan worden gebruikt om 3 tot 5 (C)PE-punten te claimen bij vakorganisaties als ISACA, ISC2 en NOREA. Tot aan zee!

SS@TB

Links

[1] Website: http://2016.ssatb.nl

mr. Rachel Marbus, @rachelmarbus op twitter

LET'S ENCRYPT IS IN PUBLIC BETA

Iedereen die op Internet actief is gebruikt elke dag wel een versleutelde https-netwerkverbinding (TLS, opvolger van SSL) en de privacyvoorvechters willen dat op elke website zien. Daar heeft The Electronic Frontier Foundation (EFF), een digitaleburgerrechtenorganisatie uit Amerika, een oplossing voor bedacht en die heet Let's Encrypt [1].

Samen met Mozilla, Cisco, Akamai, IdenTrust en onderzoekers van de universiteit van Michigan is Let's Encrypt ontwikkeld. De organisatie Internet Security Research Group (ISRG) is de eigenaar van de dienst en heeft als doel om financiële, technologische en educatieve belemmeringen voor een veilig internet te verminderen.
Let's Encrypt biedt gratis en eenvoudig op elke website een TLS-certificaat die in elke belangrijke browser wordt vertrouwd. Met bijna één druk op de knop heb je automatisch een sleutelpaar en certificaat voor je website. Met een klein stukje extra software op je webserver kun je automatisch geheime en publieke sleutels genereren, een Certificate Signing Request bestand maken, deze opsturen naar de Certificate Authority (CA), een getekend certificaat terugkrijgen en deze in configuratie van webserver opnemen. Geen gedoe meer met handmatige procedure, moeizame applicaties en ingewikkelde configuraties maar een hele eenvoudige installatie van een stukje software en het draaien van de software op de webserver zelf.
Met certificaten kun je ook 'Perfect Forward Secrecy' [2] op de webserver instellen. Naast Let's Encrypt kun je deze bestellen bij Symantec of QuoVadis. Verschil is alleen dat ze niet gratis zijn maar wel meer mogelijkheden, flexibiliteit en vertrouwen bevatten. Je kunt die certificaten bijvoorbeeld ook op servers zetten die niet op Internet aangesloten staan en het hogere vertrouwen is ingeregeld doordat ze bij aanvraag van certificaat de organisatie valideren of Extended Validation (groene balk in browsers) certificaten aanbieden (Let's Encrypt biedt alleen Domain Validation voor de certificaten). Daarnaast heb je met Symantec- of QuoVadis-certificaten meer technische kennis nodig want die bieden geen software om automatisch sleutels op de server te genereren en certificaten aan te vragen. Voor bedrijven is hoger vertrouwen belangrijk en zijn de kosten van dat soort certificaten (rond de €500,- per jaar) meestal wel op te brengen.

Certificaatvertrouwen

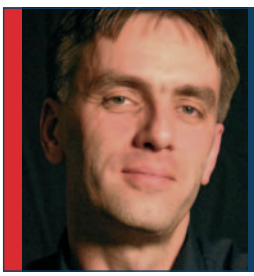
Het vertrouwen van een CA is van levensbelang voor het uitrollen van TLS-certificaten. Dit heeft Let's Encrypt verkregen door zich als een Intermediate CA te laten ondertekenen door de al vertrouwde Root CA 'DST Root CA X3'. Dit is een Root CA die door het CA/B Forum is geaccordeerd en hierdoor is opgenomen in de Trust Stores van o.a. Microsoft, Apple en Mozilla voor zowel desktop als smartphones. Met dit vertrouwen zijn Let's Encrypt-certificaten te gebruiken in Internet Explorer, Edge, Chrome, Firefox en Safari. Ook in veel andere browsers worden de certificaten van Let's Encrypt vertrouwd.
Om het vertrouwen te krijgen, dient men wel aan veel eisen voldoen. Daarvoor is het Certificate Practice Statement (CPS) en de Certificate Profile (CP) opgeleverd en zijn de nodige audits uitgevoerd. Deze audits zijn niet alleen op de CA zelf uitgevoerd maar ook op het gebruikte certificaat uitgifte protocol, Automatic Certificate Management Environment (ACME) en de software voor de webserver.

Het ACME-uitgifteprotocol

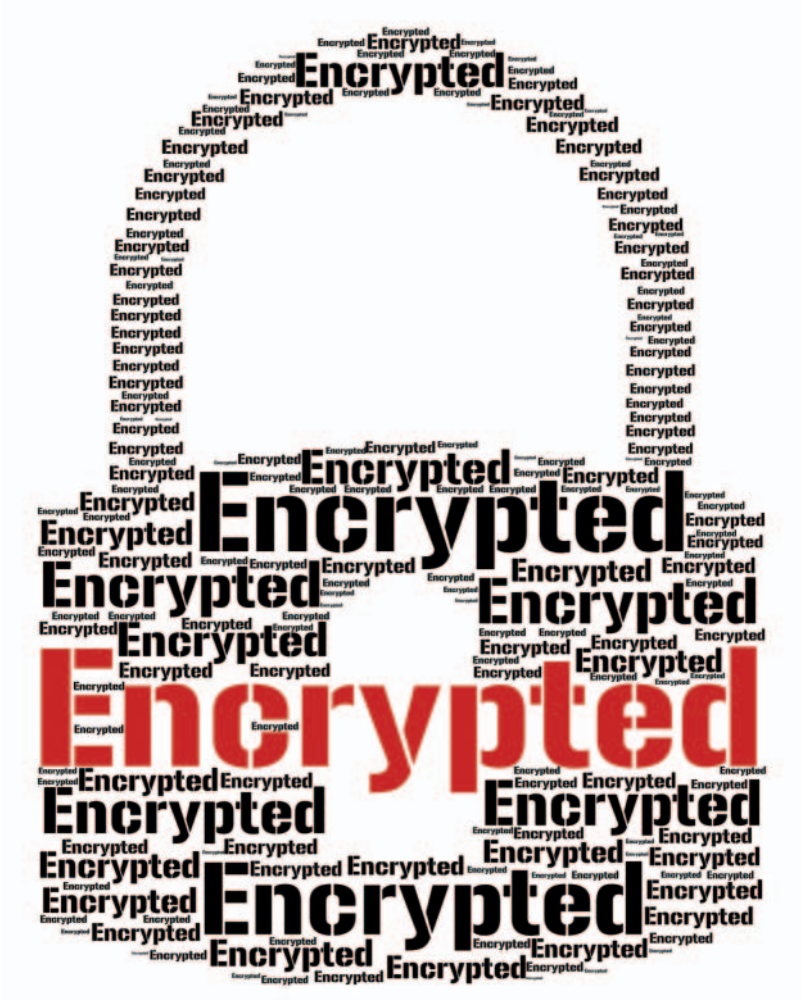
De certificaat uitgifte draait rond het ACME-protocol waarin de standaardfuncties zijn opgenomen. De certificaatfuncties, sleutels genereren, certificaat aanvragen, vernieuwen en intrekken zitten ingebouwd in de Let's Encrypt-software en kunnen automatisch uitgevoerd worden. Het ACME-protocol staat geregistreerd bij het IETF en heeft op dit moment de status 'Internet-Draft'.
ACME kan niet omgaan met Wildcard-certificaten en je zult altijd een volledige naam moeten gebruiken. Dit heeft te maken met het authenticatiemethode van uitgifte van certificaten want er wordt o.a. gecontroleerd of het certificaat aangevraagd wordt vanaf de webserver waar de website daadwerkelijk draait.

De Let's Encrypt-Software

De Let's Encrypt-software is open source en geschreven in Python. Op GitHub is de software te vinden en kun je het downloaden om het op je eigen website te gebruiken. Op dit moment wordt Let's Encrypt alleen ondersteund op Unix-like OS's en indien je Apache (webserversoftware) hebt draaien op een Unix-like OS, kun je het volledig automatisch uitvoeren. Met andere webserversoftware kun je de certificaten wel aanvragen maar niet automatisch doorvoeren.



Harld Röling is werkzaam bij de afdeling CISO van een Nederlandse bank en heeft zich vanaf 1999 gespecialiseerd in de technische en organisatorische aspecten van asymmetrisch Key Management en PKI. Daarnaast is Harld vrijwilliger bij Bits of Freedom voor Privacy Cafe's en de Toolbox. Harld is bereikbaar op e-mailadres harld.roling@hroling.nl.



Eén druk op de knop geeft je automatisch een sleutelpaar en certificaat voor je website

Op Debian gebaseerde OS's zoals Debian zelf en Ubuntu is de software volledig automatisch te gebruiken. Op Windows is het nog niet volledig te gebruiken maar zijn er wel PowerShell-modules die het succesvol kunnen laten draaien.
De Let's Encrypt-software moet draaien op de webserver waar de website op draait. Je kunt niet op een andere server de certificaten aanvragen en daarna kopiëren naar de webserver. Tevens moet de webserver bekend zijn in de DNS omdat daarop een controle uitgevoerd wordt.

Sleutels genereren en certificaat aanvragen

Bij het draaien van de software bekijkt deze de lokale server en zoekt de configuratie van de webserver die daarop draait. Indien deze gevonden zijn kun je de keuze maken voor welke website je een certificaat wilt hebben en wordt er een sleutelpaar genereerd, een Certificate Signing Request (CSR)-bestand gemaakt en opgestuurd naar Let's Encrypt. Het CSR wordt dan door de CA gecontroleerd, ondertekend en teruggestuurd naar jouw webserver. De Let's Encrypt-software zorgt ervoor dat de webserverconfiguratie aangepast worden en de webserversoftware wordt opnieuw opgestart.
De geheime sleutels worden op de webserver zelf gegenereerd en blijven ook alleen op de server staan. Deze worden niet naar Let's Encrypt gestuurd.
Bij het vernieuwen van de certificaten wordt er een nieuw sleutelpaar gegenereerd zodat je elke keer een nieuwe sleutel op de website krijgt. Een Let's Encrypt-certificaat kun je door dezelfde software automatisch laten vernieuwen zonder dat je iets moet doen op de server.
Limiet is op dit moment maximaal vijf certificaten per domein per week. Wil je er meer dan zal je dat goed moeten plannen en het verdelen over meerdere weken.

Intrekken en valideren

Een van de belangrijke onderdelen van sleutels en certificaten is dat ze beperkt geldig zijn en indien de sleutels gestolen

worden, de certificaten ongeldig gemaakt kunnen worden. In PKI-termen noemen ze dat intrekken of revoken.
Dat intrekken is ingeregeld en je kunt certificaten ongeldig verklaren en controleren met de Certificate Revocation List (CRL) of met het Online Certificate Status Protocol (OCSP). Hiermee is de PKI van Let's Encrypt compleet en zijn alle lagen ingeregeld. CRL en OCSP zijn openbaar zodat iedereen deze kan raadplegen als men het certificaat wilt gebruiken.
Intrekken van eigen certificaten kun je ook uitvoeren met de software van Let's Encrypt. Na het intrekken van jouw certificaat, kun je de status via CRL of OCSP opvragen. De URL van de CRL en OCSP-server zit in elk uitgegeven certificaat.

Geldigheidsduur

In de Public Beta zijn certificaten drie maanden geldig en indien je in de server een script maakt dat elke drie maanden het certificaat automatisch vernieuwt, is dat geen probleem. Hiervoor is wel een configuratiebestand nodig waar de nodige instellingen zijn opgenomen. Voor elke website kun je dan automatisch een certificaat laten vernieuwen en de webserver wordt na ontvangen van certificaat even opnieuw gestart. Dat laatste heeft impact op de gebruikers want die verliezen dan hun actieve sessie.
Ook kun je één certificaat maken voor alle websites die op de specifieke machine draaien. Het is mogelijk om één certificaat aan te maken met bijvoorbeeld vijf of meer websites. De websites worden dan opgenomen in het veld 'Subject Alternatieve Name' in het certificaat.

Hash-algortime en sleutellengte

Uitgegeven certificaten zijn SHA-256 gebaseerd zodat ze voldoen aan de laatste eisen en standaard algoritmen. Indien je nog websites hebt draaien met een SHA-1-certificaat kun je met Let's Encrypt heel eenvoudig een update doorvoeren en is de site ook na de SHA-1-blokkade van juli 2016 nog beschikbaar. Sleutellengte is standaard RSA 2048 bits maar een sleutel van RSA 4096 bits is met één optie in de applicatie in te stellen. Meer keuzes zijn er op dit moment niet mogelijk maar ze zijn bezig om ook Elliptic Curve Cryptography (ECC) in de software toe te voegen.

Certificate Transparancy

Certificate Transparancy (CT) is een systeem dat men alle uitgegeven certificaten kan inzien. Let's Encrypt heeft dit ook ingeregeld en alle certificaten die door Let's Encrypt zijn uitgegeven zijn publiek in te zien en te achterhalen.
Met CT kan iedereen achteraf controleren welke certificaten er uitgeven zijn door welke CA. Het is een controle achteraf en indien er toch een foutief certificaat uitgeven is, kan deze ingetrokken worden. Dit is wel een onderwerp om over na te denken want wil je zeker dat bepaalde sites publiek bekend zijn?

Certificate Transparency laat iedereen achteraf controleren welke certificaten er uitgeven zijn

Conclusie

Let's Encrypt brengt de mogelijkheid van een versleutelde verbinding binnen handbereik van iedereen die een eigen webserver heeft. Voor de thuis websites, kleine testomgevingen, demo-websites en andere soorten web-omgevingen is het zeker de moeite waard te onderzoeken of Let's Encrypt tot de mogelijkheden behoort. Mensen die geen kennis en kunde hebben van certificaten kunnen hiermee zelfs aan de slag.
De geldigheidsduur van de certificaten is wel een aandachtspunt en de termijn van drie maanden kan een probleem zijn als je dat niet goed bijhoudt. Daar zal je dus iets voor moeten opzetten en inplannen dat het of automatisch gaat of dat je het elke drie maanden handmatig uitvoert.
Voor grote corporate websites is het niet zo geschikt om Let's Encrypt te gebruiken en dat is ook niet de doelgroep van Let's Encrypt. De functies zijn zakelijk zeer interessant want PKI zal ook binnen eigen netwerken komende jaren een belangrijk onderwerp worden. En mobile devices krijgen steeds vaker apps die device-binding eisen en daar zit regelmatig een PKI-onderdeel in. Automatisch certificaatbeheer is met dit concept een stuk eenvoudiger in te regelen.
Al met al is Let's Encrypt een welkome aanvulling een open en onbetrouwbaar netwerk als het internet is. Criminelen, overheden en bedrijven hebben geen mogelijkheid meer om de netwerken af te luisteren.

Links

[1] Website van Let's Encrypt: https://letsencrypt.org
[2] Harld Röling (2016). Perfect Formward Secrecy op jouw website. Informatiebeveiliging 2016-1, 16-17.

Door Lex Borger, hoofdredacteur Informatiebeveiliging, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl

STRUCTUUR, INHOUD, VORM, ANALYSE

Titel: SIVA
Subtitel: Methodiek voor de ontwikkeling van auditreferentiekaders
Auteur: Wiekram Tewarie
Met medewerking van: Eline ter Meer en Eric Nieuwland
Taal: Nederlands
Pagina's: 222
Uitgever: VU University Press
Datum: April 2014
ISBN: 9789086596706

Deze review gaat over een boek voor auditors. Of is het een boek voor informatiebeveiligers? Of zelfs voor alle IT-ers? Dat laatste gaat waarschijnlijk een beetje ver, maar de SIVA-methodiek is voor een veel grotere groep bruikbaar dan voor auditors alleen. Daarom helpt het dat er een toegankelijk boek beschikbaar is om deze groep met de methodiek bekend te maken.

Ik ben dit jaar bewust geworden van het SIVA-gedachtengoed. Ik kende het al, zo bleek. Het boek dat Wiekram Tewarie vorig jaar publiceerde [1] is gebaseerd op zijn wetenschappelijk onderzoek, waarvan de thesis ook bij de VU is gepubliceerd [2]. Toen was 'SIVA' nog niet de naam van dit gedachtengoed, het wordt met 'SCF-framework' aangeduid (Structure, Content, Form and M3), ook in het artikel dat Wiekram met o.a. Ronald Paans in de IT Auditor hierover schreef [3]. Ook het NCSC gebruikte dit raamwerk al, in hun richtlijnen voor webapplicaties en mobiele apparaten [4]. In de vernieuwde uitgave van de richtlijnen voor webapplicaties wordt er expliciet naar SIVA verwezen [5]. Het Centrum Informatiebeveiliging enPrivacy (CIP) publiceerde een hele reeks documenten over 'Grip op Secure Doftware Development (SSD)'. Het normenkader hiervan is volgens SIVA beschreven. De Auditdienst Rijk (ADR) en ICTU gebruiken SIVA. En impliciet gebruiken de lezers van de NCSC-richtlijnen en de CIP-SSD-beveiligingseisen ook SIVA. De methode neemt dus een grote vlucht, vooral binnen het rijksoverheidsdomein, maar sijpelt door in andere domeinen.

Het boek behandelt de vier methodische hulpmiddelen, die samen SIVA spellen. Ik tracht deze heel kort weer te geven:

- S voor structuur - kijken naar de structuur rond een systeem, inclusief de invloed van de omgeving, wat resulteert in vijf lagen
- I voor inhoud - het bekijken van het systeem vanuit verschillende invalshoeken: doel, functie, gedrag, structuur. Hiermee worden ook verschillende abstractieniveaus aangepakt
- V voor vorm - normcriteria dienen compleet te zijn. Door ze in een vaste vorm te formuleren dwing je jezelf om compleet te zijn
- A voor analysevolgorde - bekijk een systeem niet alleen in isolatie, maar ook in zijn omgeving. Werk hierbij top-down én bottom-up

Ik voel me bevoorrecht dat ik met Wiekram samen heb mogen werken aan het opzetten van een aantal normen volgens de SIVA-methodiek. Dan kun je met de meester zelf discussiëren over de toepassing van de methodiek. Als security architect vielen mij paralellen op met de SABSA methodologie, al zijn SIVA en SABSA zo verschillend van insteek dat een afbeelding van de een op de ander niet eenvoudig te maken is. De kolommen en rijen van de SABSA-matrix zijn niet zomaar te projecteren op een van de dimensies in SIVA. Dat is dan een onderwerp voor een apart artikel…

De SIVA-methodiek toepassen is in beginsel moeilijk. Het is logisch opgezet, maar dat wil niet automatisch zeggen dat het zomaar toe te passen is op je eigen dagelijkse praktijk. Er zijn keuzes te maken die niet voor de hand liggen. Soms handel je naar eigen beste inzicht en verkrijg je een werkbaar resultaat voor jezelf, wat niet door andere sleutelpersonen herkend wordt. We hebben collectieve ervaring nodig met de methodiek. Daarom is de toepassing door het NCSC wel de meest belovende inzet ervan. Als we die voorzet in onze omgeving gebruiken en bewerken naar volledige criteria dan groeit die collectieve ervaring vanzelf.

Links

[1] SIVA boek: http://vuuniversitypress.com/catalogus#!/SIVA-Methodiek-voor-de-ontwikkeling-van-auditreferentiekaders/p/36808065
[2] Wiekram Tewarie's thesis: http://vuuniversitypress.com/catalogus#!/A-Structured-Approach-to-IT-Auditing/p/15496909
[3] Artikel in IT-Auditor: http://www.deitauditor.nl/beroepsontwikkeling-reglementering/het-construeren-van-referentiekaders-een-principle-based-aanpak/
[4] NCSC-richtlijn mobiele apparaten: https://www.ncsc.nl/actueel/whitepapers/-beveiligingsrichtlijnen-voor-mobiele-apparaten.html
[5] NCSC-richtlijn webapplicaties: https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-vernieuwde-ict-beveiligingsrichtlijnen-voor-webapplicaties.html
[6] CIP-beveiligingseisen Grip op SSD: http://www.cip-overheid.nl/downloads/grip-op-ssd/

EMERGENT

SABSA thinking is based heavily on systems engineering concepts. We see the enterprise itself as a system of systems, hierarchically complex, with layered tiers of sub-systems and component interactions at every level of decomposition and abstraction. Systems are designed to have certain functionality to meet the system requirements, and in SABSA we articulate these requirements and functional properties through a series of Business Attributes. However, there are often properties of complex systems that were not designed, but which we discover once we operate and use the system. These are called 'emergent properties'.

An emergent property is unexpected during the design phase, but emerges once we operate the system. The Attributer sees the most generic emergent property as being 'entropy', the level of disorder in a system. All systems have a certain level of entropy. The second law of thermodynamics tells us that the entropy of a given system undergoing a real process will tend to increase over time (increasing disorder) and that to correct this tendency we must do 'work' to restore the desired order. This law of physics applies to all systems at all levels of scale, from the universe itself down to any natural or man-made microsystem. For best results we consider a system in the context of its eco-system – the system and its environment.

For those of you that have kept a garden, it is a familiar experience. You do work on your garden to make it orderly. You trim the hedges, mow the lawns, pull the weeds, deadhead the roses, sweep the paths and it looks great. You go away on two weeks holiday and when you return it looks like a jungle again. The natural processes have created chaos out of order, and you need to do a whole lot of work again to restore the order. That's the second law of thermodynamics in action.

The attribute 'emergent' is not part of our design requirements, but is one that we will experience anyway, and therefore we must design to handle it. Examples of unwanted emergent properties are unsafe system behaviour and insecure system behaviour. These behaviours arise from unforeseen interactions between system components. They are not properties of the components themselves, and only emerge during component interactions. For example, a transport network carries traffic of some type either physical (such as cars and lorries) or logical (such as digital packets in a communications network). The components of the network are the traffic items, the transmission paths and the routing mechanisms. An unwanted emergent property of a network is 'traffic congestion'.

In computer systems we see countless examples. A disk storage system will become fragmented and periodically will need work to defragment the disk. A computer system can be configured with all the parameters set to meet a standard configuration, but in time this will degrade as minor changes are made, applications are run, patches are applied, and so on. It needs periodic review and reconfiguration to keep it to the standard settings.

When we turn to the subject of cyber security, the potential for degradation and entropy increase is well beyond previous experience with physically contained computer systems. Operating a secure cyber system in the eco-system called cyberspace is very challenging. Cyberspace is a complex system of systems that grows and changes all the time. It definitely has a time dimension and is therefore subject to the second law, but it has no physical spatial dimensions or restrictions. The potential for emergent properties is infinite. We have never before faced this challenge and most people are struggling to get their minds around the concept of cyberspace and hence cyber security.

Whilst we focus on securing the components of cyberspace we will never get control over cyber security. Only be stepping back and taking a systems engineering view, including the concept of emergence, will we ever stand a chance of being successful. This requires a complete change in mind-set. It requires SABSA thinking.

The Attributer

VERSLAG CISO 9

VEILIG IN DE CLOUD?

Bart van Staveren opende deze middag met een eigen ervaring. De aankoop van een nieuwe computer leverde hem een reeks aanbiedingen op van bedrijven voor gratis dataopslag in de cloud. De cloud is dus een populair onderwerp waarvan velen willen profiteren. Maar hoe handig en veilig is dat allemaal? Daar gingen wij het over hebben.

Evidence Based Trust

Dat is wat de Cloud Security Alliance (CSA) wil bieden. Reinier Landsman Voorzitter van de CSA Netherlands Chapter, legde uit hoe deze non-profitorganisatie tracht te bouwen aan best practices voor een 'trusted cloud ecosystem' voor security assurance (zekerheid) voor Cloud Computing. Daarnaast zijn bewustwording, transparantie en een raamwerk voor control, belangrijke speerpunten. Wereldwijd worden bijeenkomsten georganiseerd die vrij toegankelijk zijn.

Reinier Landsman

Gebruik maken van de cloud vergt nadenken. Wat zijn de risico's die samenhangen met de soort data en de wijze van verwerking? En pas op: Smog is geen cloud!

Reinier besprak de issues die behoren bij 'trust', de verantwoordelijkheden van cloud-service-provider en die van de end-user-organisatie. Vanzelfsprekend maakt het verschil of er een MKB-organisatie of een groot concern in het spel is. CSA wil de MKB-er ontzorgen door haar activiteiten.

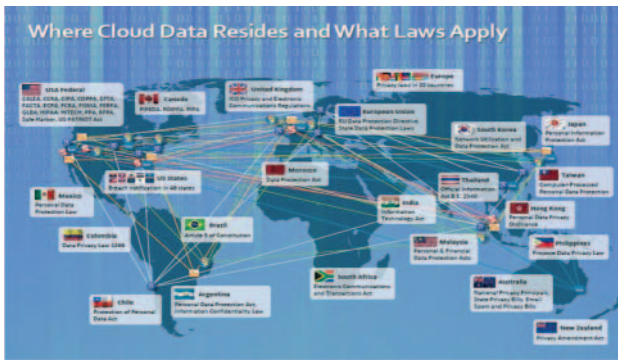
Belangrijke aandachtspunten zijn, de wet- en regelgeving die lokaal en specifiek is en de verschuiving van de dreigingen naar datagerelateerde incidenten. De kernvraag voor CSA is "hoe realiseren en optimaliseren wij een vertrouwde transparante en veilige cloud?"

SMOG = Situations Managed Outside of Governance

Tenslotte gaf Reinier een overzicht van de CSA-producten waaronder de Cloud Control Matrix met 130 controls verdeeld over 16 domeinen en het CSA-STAR-register waarbinnen bedrijven zich kunnen meten en certificeren op de mate waarin hun diensten voldoen aan de normen van de Secure, Trust, Assurance Registry.

Cloud, the future of IT services and the next level of quality control

De titel van de bijdrage van Peter van Eijk aan deze middag gaf al direct de ambitie van Peter aan: verder denken dan aan voor de hand liggende antwoorden. Hij gebruikte een ondertitel om de toekomstige zorg om



Cloud control matrix

kwaliteitsborging te onderstrepen, "Ownership and control of IT in the cloud supply chain". Het gaat om een ontwikkeling die op gang is gekomen en niet meer wordt gestopt. Zijn uitgebreide ervaring als trainer bleek uit de snelle en gerichte manier waarop hij zijn verhaal onder onze aandacht bracht.

Peter van Eijk

Aan de hand van een aantal voorbeelden schetste Peter transformaties die in het verleden plaatsvonden waardoor de IT weer in een nieuwe fase terecht kwam. Hierbij sneuvelden dan bestaande technieken en oplossingen. Daarom noemde hij die transformatie disruptive, het vervangen van iets waaraan wij gewend zijn. Hij stelt vast dat hard- en software steeds maar goedkoper worden en de netwerken en componenten steeds sneller worden. Tegelijkertijd vergt het steeds meer moeite om nog enigszins iets van beveiliging te realiseren. Zijn conclusie is dan ook dat individueel iets regelen onmogelijk is.

De cloud is een nieuw model voor het leveren van diensten, gebaseerd op dienstverlening door derden. Dit leidt tot nieuwe businessmodellen met eigen karakteristieken en nieuwe risico's. Daarbij zijn de winstkansen de grote prikkels om over te stappen op de nieuwe mogelijkheden.

Peter liet zien hoe de keten van de dienstverlening in IT in elkaar steekt. Daarbij is de kernvraag: "wie is in control?" De vele gebruikersgroepen werken op basis van verschillende principes. De cloud biedt de mogelijkheid om de verdeling anders in elkaar te steken, wat doe ik zelf, wat doet een ander? Voor een antwoord op deze vraag is het noodzakelijk dat een duidelijke grens wordt gemarkeerd. En daarmee kan de essentie van security worden aangepakt: wie doet wat? Bijvoorbeeld: wie doet de updates, wie doet de scaling van hardware en wie patcht het OS? De topvraag luidt:

"What do I do, what do you do, and what do I do, if you don't?" Samenwerken dus.

Peter gaf een overzicht van de elementen van cloud-security, van de 'chain of control' en van de manier waarop deze onderwerpen in de CSA-producten zijn verwerkt zodat de theorie kan worden omgezet in een uitvoerbare praktijk.

Discussie

In de discussie kwam een aantal onderwerpen ter sprake die typisch zijn voor beveiliging. Wat te doen met de claims van providers over hun staat van beveiliging. Hoe is dat te controleren? Er zijn de variaties in controls aan de ene kant en aan de andere kant de mate van transparantie. In hoeverre laat de provider in zijn keuken kijken? Een compliance-vraag. Encryptie lijkt een belangrijke maatregel bij het opslaan en transporteren van data. Maar wat te doen tijdens de bewerking als die in de cloud plaats vindt? Er is dus nog wel wat te doen op het gebied van beveiliging. Internationale uitwisseling van gegevens stuit direct op het privacyvraagstuk. CSA probeert politieke stellingname te vermijden en zich te richten op de functie van discussieplatform. Daar kan waarde worden toegevoegd. Van belang is het segregeren van data. Dat wil zeggen, data zoveel mogelijk voor een enkele functie benutten. Dat vereenvoudigt het beheer van de gegevens. Een gevolg daarvan is wel dat de hoeveelheid data toeneemt hetgeen ook weer een beheerprobleem oplevert. Nog een keer kwam aan de orde dat cloud betekent: nieuwe functies. Dus de vraag: "wat moet ik anders gaan doen?" bepaalt waar de 'knip' ligt tussen wat wij en wat zij doen. Dat vergt vertrouwen (van twee kanten) en de deskundigheid SLA-afspraken en de uitvoeringspraktijk daarvan te kunnen beoordelen.

Interessant was de praktijkervaring dat veel organisaties geen goed idee hebben van het aantal clouddiensten dat wordt afgenomen.

CSA zorgt voor een terminologie en gereedschappen die partijen kan helpen om afspraken mogelijk te maken terwijl de partijen hun eigen verantwoordelijkheid en zelfstandigheid behouden. Standaarden en methodes die al beschikbaar zijn worden gebruikt. Alleen de gaten die er zijn, tracht CSA op te vullen. Voorschriften geeft zij niet en iedereen is welkom om mee te doen. De ontwikkelingen gaan snel en zijn met regels niet bij te houden. Dat vraagt om een flexibele aanpak met een direct en snel contact op onpartijdige en deskundige wijze.

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

APPLE SAFE?

De FBI wil dat Apple een speciale versie van iOS maakt voor de iPhone die door Syed Farook gebruikt werd. Apple weigert, met als reden dat deze speciale versie de FBI een springplank zou geven om dit bij meer apparaten toe te passen. Verder schept het natuurlijk een juridisch precedent en we komen er in de rechtbank achter dat de FBI in het begin van het onderzoek kennelijk een domme zet gedaan heeft door de AppleID van Syed te laten resetten.

De beveiligingswereld heeft zich zo goed als unaniem achter Apple geschaard. We klagen als informatiebeveiligers vaak over de geslotenheid van Apple en iOS, maar in dit geval beschermt het toch de vrijheid. Wijlen rechter Antonin Scalia zei al: "There is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."

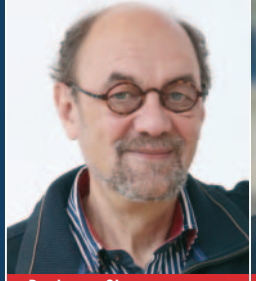
We zullen zien hoe dit zich verder uitspeelt. Zou er een formeel protocol moeten zijn waarmee de gevraagde informatie verstrekt wordt? Kan dit ook? Willen we dit? Hoe balanceren we criminaliteit versus privacy? De redactie reageert.

Maarten Hartsuijker

Er was eens een bedrijf dat kluizen verkocht. Iedereen wilde de kluizen van het bedrijf graag kopen. Ze waren niet alleen mooi en hip om te zien, maar je kon er ook heel veilig je spullen in bewaren. Zo veilig, dat je zeker wist dat niemand je spullen kon stelen. Zelfs de maker van de kluis niet. Zo'n kluis was erg gewild bij iedereen die zijn spullen tegen inbrekers wilde beschermen.

Omdat sommige mensen bewijzen over misdaden in hun kluis bewaarden vond de overheid dat de maker van de kluis zijn producten minder veilig moest gaan maken. De kluizen moesten met een loper op afstand geopend kunnen worden. Dat vervolgens veel medewerkers van de kluizenfabrikant, grote groepen ambtenaren en onvermijdelijk ook criminelen in de kluis van iedereen konden komen, tja, dat was helaas niet anders. Maar een kluizenfabrikant met achterdeurtjes in zijn kluizen is natuurlijk geen lang leven beschoren. Niemand koopt een kluis waarvan anderen de sleutel hebben...

Als je als consument een product koopt, moet je ervan opaan kunnen dat dit product veilig is. Met het bewust verzwakken van producten tref je alleen de massa. Slimme criminelen zullen zichzelf met andere middelen gaan beschermen terwijl nietsvermoedende consumenten door de aangebrachte


Bart van Staveren


Lex Borger


Maarten Hartsuijker

kwetsbaarheden meer risico lopen om slachtoffer te worden van computermisbruik.

Tegelijk moeten we ons als beveiligers naar mijn idee niet teveel laten afleiden door dit soort berichtgeving. Er is Amerikaanse bedrijven, met de Snowden en Safe Harbor-fiasco's nog vers in het geheugen, veel aan gelegen om de rest van de wereld het idee te geven dat gegevens veilig bij ze zijn. En Apple doet in deze rechtszaak erg zijn best om dat te benadrukken. Maar het feit dat het bedrijf blijkbaar in staat is om zonder tussenkomst van de gebruiker een compleet OS te vervangen terwijl daarbij de encryptiesleutels en de data in tact blijven, zou al enkele wenkbrauwen moeten doen fronsen. Daarnaast moet ik ook nog wennen aan het feit dat deze overheid, met vele slimme koppen in dienst en grossierend in software van bedrijven als Hacking Team en Vupen, niet in staat is om via een kwetsbaarheid toegang tot de data te krijgen. Zou mijn iPhone dan echt de holy-secured-grale onder de telefoons zijn? Ik hoop het.

Bart van Staveren

Als informatiebeveiligers adviseren we onze opdrachtgevers hun gegevens goed te beveiligen ook op mobiele apparaten, die ze aan hun werknemers verstrekken.
Als zij dit niet doen kan dat grote bedrijfsschade of reputatieschade tot gevolg hebben. Privacywetgeving stelt organisaties aansprakelijk bij het verlies van gegevens en overheden kunnen ook boetes opleggen. En gelukkig zijn er nu leveranciers die standaard de vereiste functionaliteit bieden. Dat ook criminelen en terroristen hier gebruik van maken, is vanuit hun standpunt niet meer dan vanzelfsprekend. En hier heb je dus het dilemma. Het publiek belang eist van de overheid dat ze misdaad bestrijdt. Hetzelfde publiek belang eist van de leverancier de garantie dat zij beveiligingsfunctionaliteit levert die niet door derden (waaronder de overheid) doorbroken kan worden. De eisen van de misdaadbestrijders aan in dit geval Apple lijken op het eerste gezicht heel redelijk en logisch. Wanneer de overheid dezelfde vraag zou stellen om achter bedrijfsgeheimen te komen van een organisatie in een bevriend land zouden we er schande over spreken. Wat de uitspraak in de Syed Farook case ook zal zijn, ik denk dat het laatste woord over dit dilemma voorlopig nog niet op papier is gezet.

Lex Borger

Deze zaak heeft vele mogelijke invalshoeken, die echter allen uitkomen op dezelfde conclusie: Apple heeft gelijk. Een aantal noem ik hier:

Kun je de FBI dit onderzoek nog wel laten voortzetten? Ze hebben al met bewijs gerommeld door het AppleID te laten resetten. Voor dit soort zaken moet er een protocol zijn en dat protocol moet vanaf de eerste seconde gevolgd worden. De pairing van de iPhone met dit AppleID verstoren was stom. Punt uit.

Syed had hun privételefoons vernietigd. Wat verwacht de FBI aan te treffen op de werktelefoon? Deze terrorist heeft al duidelijk gemaakt dat hij beveiligingsbewust is.

Wat het betekent om een speciale versie van iOS maken moet niet onderschat worden. Dit zal in het geheim moeten, want je wil het niet laten lekken. Je moet het goed testen, want het mag niet de forensische integriteit van de telefoon ter discussie stellen. Je moet het documenteren en die documenten overgeven aan de FBI. Tegelijkertijd wil je voorkomen dat de FBI middels code-analyse achterhaalt wat Apple gedaan heeft. Ik zou niet weten hoe je aan al deze eisen tegelijk kunt voldoen.

Mag de Amerikaanse rechter hier wel over oordelen? Apple verkoopt wereldwijd, en een succes van de FBI wordt in Chinese en Russische kringen straks gebruikt om hetzelfde van Apple te eisen, nu met de wetenschap dat het gaat om software die bestáát. De eerste horde is dan al genomen. Op zijn Amerikaans: 'The cat is out of the bag'.

Op het moment van mijn schrijven is de publieke opinie aan het omslaan. Dit heeft zijn redenen. De gewone mens kan de gevolgen voor de veiligheid van alle iPhones niet bevatten. Gemeten naar menselijke maatstaven voelt het weigeren van Apple niet goed. Er is een vreselijke moordpartij geweest en wellicht missen we informatie door Apple's weigering. De nagedachtenis aan de slachtoffers is krachtig. De collectieve emotie is dat de man áchter deze aanslag ook gepakt moet worden.

De publieke opinie werkt hier dus niet bij. Apple heeft aangegeven zich te willen schikken naar de uitspraak van een panel van experts, die deze problematiek wél kunnen begrijpen en overzien. Hiermee trekken ze het dan uit de politiek.

Apple zou niet in de positie gekomen zijn waar ze nu inzitten als er niet een technische mogelijkheid was om de iPhone van nieuwe software te voorzien zonder de inhoud ervan te wissen. De FBI heeft aan de hele wereld duidelijk gemaakt dat iOS apparaten een backdoor hebben - laten we het noemen wat het is - door er toegang toe te vragen. Misschien gaan ze deze slag winnen, maar de privacy-oorlog winnen ze niet. Je kunt er donder op zeggen dat er al een team van ontwerpers bezig is om dit ongedaan te maken.

De kern van de vraag is wat we in onze samenleving willen. Kunnen we middelen inzetten om onze diepste gedachten en communicatie geheim te houden? Het antwoord is ja, met encryptie. Dan is de vraag of we dit wel mogen niet meer relevant, criminelen vragen geen toestemming. Mag een leverancier een product leveren met deze middelen ingebouwd? Ja. Mag een leverancier gedwongen worden om dit op te geven? In redelijkheid. En die redelijkheid heeft rechter Scalia goed verwoord.

Ik ben benieuwd wat er komen gaat.

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
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

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

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
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 2016
De abonnementsprijs in 2016 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

LASTIG OF SNEL

We leven in een tijd dat waarin sneller en makkelijker moet gaan. Op zich begrijp ik die wens wel, maar we gaan daar soms wel heel erg ver in. Sommige branches willen van alles makkelijker maken voor hun klanten. Trouwe lezers zullen wel weten dat ik met stomme verbazing in een aantal afleveringen heb geschreven over een branche die het steeds maar weer lukt negatief op te vallen, hoewel dit natuurlijk mijn persoonlijke beeld is. Op één punt vallen ze wel positief op, namelijk in het veranderen van een ouderwetse stoffige omgeving naar een dynamische omgeving waarbij iets meer risico's worden genomen. Werd vroeger met behulp van een handtekeningenkaart gecontroleerd of de man voor de balie daadwerkelijk Berry was, nu houd ik mijn pasje gewoon boven een kastje en ik kan mijn boodschapjes weer meenemen. Uiteraard kunnen de banken ook niet anders, want kantoren zijn er niet meer. De handtekeningenkaart zal ongetwijfeld vervangen zijn door een ander fenomeen.

Momenteel worden de bankpassen alleen beschermd met een combinatie van 4 cijfers die bovendien gemakkelijk te onthouden moeten zijn volgens veel gebruikers. 1-1-1-1 en 1-2-3-4 zullen ongetwijfeld veel voorkomende pincodes zijn. Een bankrekening kan leeggehaald worden wanneer je in het bezit bent van die vier cijfers. Geld overboeken moet ook steeds sneller. Een TAN-code toegezonden krijgen op je telefoon wordt als gemakkelijker ervaren dan het gebruik van een calculator om je betaling te kunnen uitvoeren en wordt als voldoende beveiliging gezien.

Het zal niemand verwonderen dat bendes de bankpas in combinatie met de pincode nog steeds het meest plezierig vinden voor hun dubieuze activiteiten. De phishing-emails komen met grote regelmaat binnen en lijken over het algemeen bedrieglijk echt. Taalkundig zijn ze niet altijd honderd procent in orde en de afzender is vaak wel als verdacht te herkennen door eens kritisch naar het emailadres van de afzender te kijken, maar uit de verhalen blijkt dat het de bendes toch vaak lukt om op die manier de spaargelden van iemand binnen te krijgen.

Zijn die mensen allemaal naïef door hun gegevens zo gemakkelijk te verstrekken? Nee, dat zijn ze niet. Vaak zijn wij juist niet bekend met de risico's of zijn we bang dat we de volgende keer bij de Albert Heijn niet kunnen pinnen en de hele rij dat kan zien. "Laten we dan tóch maar de instructies in de email uitvoeren", denken we dan.

We zitten nu in een tussenfase waarin de banken proberen om het ons nóg gemakkelijker te maken met contactloos betalen. Het gaat erg snel, maar het brengt risico's met zich mee. Iemand kan de contactloze betaling activeren door een kastje dicht bij je portemonnee te houden. Laat mij gewoon betalen met mijn telefoon, waarbij eerst ook een ingewikkelde code ingevoerd moet worden of mijn duimafdruk geplaatst moet zijn voordat de betaling gedaan kan worden. Verder is de telefoon een apparaat waarmee doorgaans voorzichtig mee wordt omgegaan.

Toch zegt mijn gevoel dat niet iedere telefoon daarvoor in aanmerking zou mogen komen. Indien er geen beveiligingsupdates uitgebracht worden voor een telefoon loop je natuurlijk het risico dat het risico van verlies van geld via kwaadwillende overname van je telefoon net zo kansrijk is als verlies van je portemonnee. Er is wel een belangrijk verschil tussen portemonnee en telefoon: de portemonnee is doorgaans minder goed gevuld dan de bankrekening.

Tja, ik ga dan toch liever voor de lastige variant, al weet ik niet of er naar mij geluisterd gaat worden.

Berry

TSTC

ICT en Security Trainingen

TSTC is een gerenommeerd IT opleidings-instituut en erkend specialist in informatie-beveiliging- en cybersecurity trainingen.

Security professionals kunnen bij TSTC terecht voor bijna vijftig security trainingen op zowel technisch als tactisch- strategisch gebied. Naast alle bekende internationaal erkende titels is het ook mogelijk diepgang te zoeken in actuele security thema's.

www.tstc.nl/security

Overzicht trainingen:

- Certified Ethical Hacker (CEH)
- CyberSec First Responder (CFR)
- Certified Chief Information Security Officer (C|CISO)

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certified Cyber Forensics Professional (CCFP)

- ISO 27001 Lead Implementer
- ISO 27001 Lead Auditor

Want security start bij mensen!!