Onderzoeksrapport

"onderzoek naar vroegtijdig bekend worden van kersttoespraak van H.M. de Koningin"

Johan de Leeuw (ABDTOPConsult)
Kees Lebon (ABD Interim)

31 januari 2013

Inhoudsopgave

Opdracht

Op kerstavond 2012 werd door een onderzoekende burger de reeds gereedstaande maar nog niet publiekelijk vrijgegeven video met de kersttoespraak van H.M. de Koningin ontdekt. In een twitter van deze burger werd de URL[1] van de kersttoespraak wereldkundig gemaakt en daarmee werd de kersttoespraak openbaar nog voordat deze formeel was vrijgegeven door de RVD en uitgezonden door de NOS.

Gezien de omvangrijke negatieve berichtgeving en het volledig willen uitsluiten van een soortgelijk incident in de nabije of verdere toekomst heeft de leiding van het departement van AZ besloten om een externe evaluatie van het incident en de sindsdien getroffen maatregelen te laten uitvoeren.

Het doel van het onderzoek luidt:

1. Stel vast waar procedures en/of menselijk handelen hebben gefaald. Hierbij in beschouwing nemende dat er verhoogde aandacht was voor het vroegtijdig 'uitlekken' van informatie gezien het eerdere incident met de Miljoenennota.
2. Geef een oordeel over de maatregelen die tot dusver zijn getroffen om herhaling of een vergelijkbaar incident te voorkomen. Met andere woorden is er naar het oordeel van de onderzoekers nog steeds sprake van een risicovolle situatie waarop aanvullende actie nodig is.
3. Geef eventuele aanbevelingen (technisch en/of procedureel) om herhaling in de toekomst te voorkomen.

Dit onderzoek is in opdracht van de SG van AZ, Kajsa Ollongren, uitgevoerd door Johan de Leeuw (ABDTOPConsult), die daarbij is ondersteund door Kees Lebon (ABD Interim).

Voor dit onderzoek zijn door Johan de Leeuw en Kees Lebon gesprekken gevoerd met:

- Henk Brons – DG Rijksvoorlichtingsdienst (RVD)
- Robert Wester – plv. DG Rijksvoorlichtingsdienst (RVD)
- Erik Johan den Hoedt - Directeur dienst Publiek en Communicatie (DPC)
- Ronald van Oosteroom – Manager Informatie Rijksoverheid, plv. directeur (DPC)
- Elma Voogt - Manager Campagnes & Media (DPC)
- Fred Steinweg - Afdeling Beeldcentrum Rijksoverheid (DPC)
- [redacted] - Afdeling Communicatie Koninklijk Huis (RVD)
- [redacted] - Afdeling Online Advies (DPC)
- [redacted] - Directie Bedrijfsvoering (AZ)
- [redacted] - Afdeling Beeldcentrum Rijksoverheid (DPC)
- [redacted] - Directeur Datiq BV

Tevens is gebruik gemaakt van de kennis van Fox-IT bij het beantwoorden van technische vragen van de onderzoekers.
Het onderzoek is uitgevoerd in de periode 10 januari -31 januari 2013.

[1] Een Uniform Resource Locator (URL) wordt op het Internet gebruikt om adressen van bronnen (resources) aan te geven.

Casus

De Dienst Publiek en Communicatie (DPC) is een baten-lastendienst van het ministerie van Algemene Zaken. DPC verzorgt dienstverlening op het gebied van communicatie voor de gehele Rijksoverheid. De Secretaris-generaal van Algemene Zaken is eigenaar van DPC en daarmee beheersmatig eindverantwoordelijk. De Voorlichtingsraad (VoRa) onder voorzitterschap van de Directeur-generaal Rijksvoorlichtingsdienst (RVD) is opdrachtgever en verzorgt de inhoudelijke aansturing. De RVD en de centrale directies communicatie van de departementen zijn de belangrijkste afnemers van de diensten van DPC.

Per 1 januari 2011 zijn taken op het gebied van foto en video vanuit de toenmalige projectorganisatie Overheidscommunicatie Nieuwe Stijl – een gezamenlijk VoRa-project - overgenomen door DPC. Dit heeft geleid tot de vorming van de afdeling Beeldcentrum Rijksoverheid. Het Beeldcentrum is verantwoordelijk voor het laten maken, ontvangen en verspreiden van beeld- en audiomateriaal. De hosting, de ontwikkeling en het beheer van het geautomatiseerde systeem, dat de workflow van dit proces ondersteunt, is uitbesteed aan Parkpost BV te Hilversum. Parkpost heeft een contract met Datiq BV te Schiphol-Rijk als onderaannemer. Hierbij levert Parkpost de datacentrum faciliteiten, terwijl de gebruikte hardware en software beschikbaar (hosting) wordt gesteld door Datiq, die ook de workflow (voor video presentaties) operationeel uitvoert voor het Beeldcentrum. Het informatiesysteem is ingericht op basis van de specificaties zoals beschreven bij de aanbesteding. De verantwoordelijkheid voor de beschikbaarheid van het systeem ligt bij Parkpost/Datiq conform de specificaties van de aanbesteding, terwijl de verantwoordelijkheid van de inrichting en het gebruik van het systeem bij het departement ligt.
De samenwerking en de gebruikte procesgang (workflow) van het aanleveren en opslaan van beeld en audiomateriaal leek betrouwbaar en efficiënt.
Het incident[2] met de kersttoespraak toonde echter aan dat de beveiliging van het informatiesysteem en de werkwijze onvoldoende waren en dat men zich hiervan niet bewust was.
De werkzaamheden hebben conform de gebruikelijke werkwijze plaatsgevonden.
De bewuste video is 21 december aangeleverd door de NOS.

Op kerstavond, om 19:36u, verzond Roeleveld zijn eerste tweet (zie bijlage, afb. 1 en afb. 2) over zijn vondst en was het incident geboren.

[2] Het hier beschreven incident heeft geen enkele relatie met het eerdere incident met de Miljoenennota in 2011 dat plaatsvond onder verantwoordelijkheid van het Ministerie van Financiën.

Bevindingen

Hieronder volgt een puntsgewijze opsomming van bevindingen per aandachtsgebied.

Werkproces

- Het Beeldcentrum bereidt de plaatsing voor van de video. Het Beeldcentrum converteert de video, kent een URL toe en plaatst de video na uitzending op Youtube;
- Bij de voorbereidingen voor het beschikbaar stellen van de kersttoespraak van H.M. de Koningin zijn de reguliere procedures gehanteerd en is niet afgeweken van deze procedures;
- De reguliere – en embargo procedure zijn niet uitgeschreven op papier. De procesbeschrijving van de werkzaamheden is summier. Vanaf het moment van aanlevering door de NOS tot aan de uitzending op 25 december om 13:00u, zijn door de afdeling Beeldcentrum een aantal werkzaamheden uitgevoerd die in een actielijst zijn vastgelegd. Dat is overigens niet hetzelfde als een daartoe strekkend protocol;
- De door de NOS aangeleverd video (vrijdag 21 december) is geconverteerd naar in totaal 6 verschillende formaten voor videobestanden. Dit dient vooraf te geschieden en vraagt enige tijd, afhankelijk van de duur van de video. In termen van uren, niet van dagen;
- Dezelfde werkwijze is door DPC toegepast als in 2011 en eerdere jaren, waarbij de video op 23 dan wel 24 december achter de schermen werd klaargezet, zodat CKH kon overgaan tot het klaarzetten en controleren van de beoogde publicatiepagina in het CMS van de Koninklijk Huis website;
- Het Beeldcentrum hanteert doorgaans een embargoprocedure bij dergelijke video's (bijvoorbeeld ook bij Prinsjesdagmateriaal), maar er is om twee redenen in dit geval van afgeweken. Vroegtijdig voorbereiden achter de schermen is noodzakelijk omdat, naar oordeel van DPC:
  a) het door de NOS aangeleverde bestand gecontroleerd zou kunnen worden voordat de video live kon op KH.nl en het YouTube-kanaal. Dat is enkel mogelijk na het doorlopen van de transcodeerstraat. Een technische controleslag dus;
  b) indertijd CKH de wens had om de videolinks voortijdig in hun CMS te plaatsen, zodat de video direct na de uitzending op televisie online kon;
- Medewerkers van Datiq zijn volledig op de hoogte van de workflow, de naamconventies en nagenoeg volledig van de content en werken als verlengstuk van de medewerkers van het Beeldcentrum;
- Het incident is niet het directe gevolg van menselijke fouten of nalatigheden tijdens de uitvoering van de workflow. Wel zou de onvoldoende beveiligde inrichting van het informatiesysteem beschouwd kunnen worden als gezamenlijk falen bij preventieve werkzaamheden.

Naamconventie

- Men had zich niet gerealiseerd dat met enig onderzoekswerk de naamconventie achterhaald kon worden (datum plaatsing, plus een opgehoogde 4-cijferige code).

Zie afbeeldingen (bijlage: afb. 3 en afb. 4). De kersttoespraak is de enige video waarvan én de gebruikte datumcode bekend is én de opdrachtgever én (na enig zoekwerk) het ID;
- Men had zich niet gerealiseerd dat wanneer de URL bekend is (gevonden is) het bestand gemakkelijk benaderbaar is;
- Bij de gebruikte naamgeving (zowel voor als na het incident) houdt men zich niet aan de Webrichtlijnen. (Denk aan: betere toegankelijkheid (voor mens en machine); betere vindbaarheid; toename in snelheid; lagere kosten voor beheer; toekomstvast (onder ander hergebruik, mobiele toepassingen));
- Gezien onderstaande logging (bijlage: afb. 6) is het aannemelijk dat de betrokken burger via de route van "trial and error" achter de bestandsnaam is gekomen en dat er zeer waarschijnlijk geen sprake is van "lekken" van de naamconventie door interne of externe medewerkers.

Beveiliging systemen, personen en audit

- In de beleving van het Beeldcentrum is de leverancier van het systeem in principe verantwoordelijk voor de beveiliging, echter deze leverancier levert alleen wat in 2010 door het ministerie van AZ is aanbesteed en gevraagd;

Uit aanbestedingsdocument MediaBank:

Veiligheid
Aangezien in de MediaBank hoogst gevoelig materiaal van bijvoorbeeld het Koninklijk Huis of het ministerie van Defensie beheerd wordt, is veiligheid een hoge prioriteit.
Het mag voor onbevoegden in geen geval mogelijk zijn om bronbestanden te benaderen op welke wijze dan ook. Ook moeten alle onderdelen van het systeem dusdanig afgeschermd worden dat enkel die delen van het systeem toegankelijk zijn, die daadwerkelijk voor de desbetreffende gebruiker bestemd zijn.
Uiteraard is het zo dat opdrachtnemende partij en betrokken personen **gevraagd** kan worden een geheimhoudingsverklaring te tekenen, om de veiligheid van niet openbaar- en embargomateriaal te borgen.
Onbevoegden (bijvoorbeeld partijen die eveneens gebruik maken van servers waarop het systeem draait) mogen op geen enkele manier toegang krijgen tot het systeem of delen daarvan.

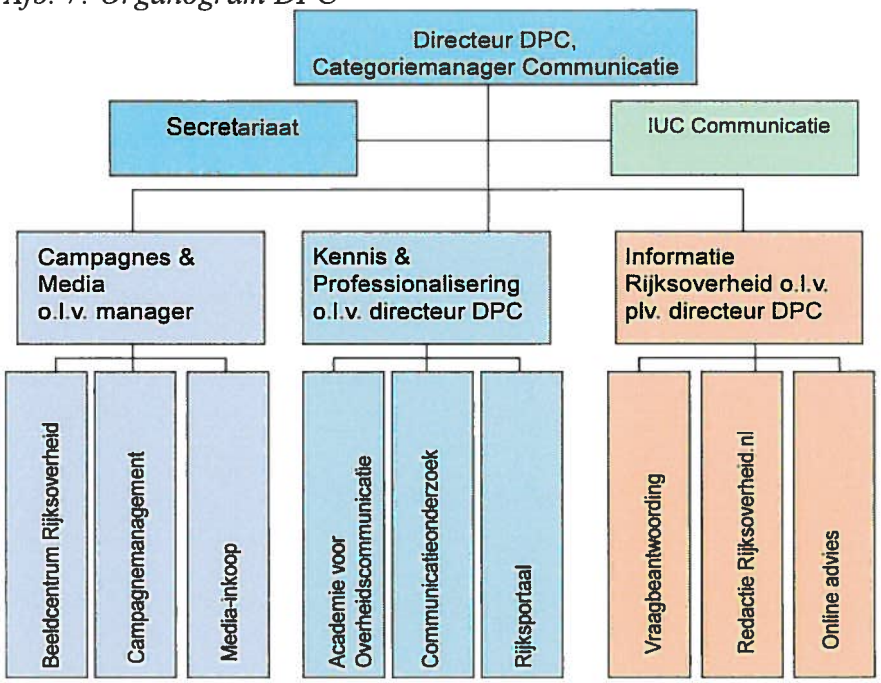
- Feitelijk moet de fysieke beveiliging van de infrastructuur liggen bij Parkpost en de logische beveiliging van het systeem bij Datiq. In het aanbestede contract wordt hier summier op ingegaan, zie kader hierboven. Geconstateerd moet worden dat zelfs de uitvoering hiervan onvoldoende is geweest. Het aanbestedingsdocument bevatte geen expliciete eisen met betrekking tot beveiliging van de hardware, software en het netwerk. Beide partijen hadden hun verantwoordelijkheid nadrukkelijker moeten oppakken. Het departement bij de opstelling van het aanbestedingsdocument en de leveranciers vanuit hun professionaliteit;
- De beveiliging van het informatiesysteem blijkt onvoldoende (geen secured server, geen DMZ[3]);
- Naar eigen zeggen heeft Datiq wel geprobeerd daar waar mogelijk proactief te reageren op onvolkomenheden binnen het informatiesysteem. In de praktijk is dat echter niet gebleken;
- Direct na het gunnen van de aanbesteding is geen VOG en geheimhoudingsverklaring van de betrokken medewerkers van Datiq ontvangen.

[3] Een demilitarized zone (afgekort: DMZ) is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. Het externe netwerk is meestal het Internet.

De medewerkers zijn ook niet gescreend. Het contract verplichtte hen daar ook niet toe. Overigens is dit ook niet door het departement gevraagd;
- Ondanks dat in het contract de mogelijkheid tot auditen van de dienstverlening van Parkpost en Datiq staat beschreven, heeft dit tot op heden nooit plaatsgevonden. Volgens zeggen werd onder audit in dit geval verstaan het verkrijgen van informatie over dataverkeer. Dat is echter niet identiek aan wat met het begrip audit wordt bedoeld. Overigens is wel inzicht in dataverkeer verkregen door "live" informatie uit het systeem;
- Waar de afdeling Online Advies jaarlijks de website Rijksoverheid.nl en gerelateerde websites laat auditen (security-audit) wordt dit niet gedaan door de afdeling Beeldcentrum voor de door haar gebruikte infrastructuur;
- Er wordt niet gewerkt conform de VIR[4] en BIR[5];
- De webrichtlijnen zijn niet toegepast (o.a. naamconventie).

Aansturing en uitvoering

Afb. 7: Organogram DPC



- De rapportagelijnen na het incident waren kort, per email en telefonisch. Het afdelingshoofd C&M is op dat moment niet geïnformeerd;
- In de periode tussen kerstavond (24 december) en 2 januari is hard gewerkt aan tijdelijke maatregelen om de Mediabank beter te beveiligen ten aanzien van toegang en inhoud;
- 2 januari wordt er voor het eerst plenair overlegd binnen DPC;
- Noch vooraf, noch achteraf is er enige betrokkenheid geweest van de plv. CIO. Niet vanuit hem zelf, noch erbij betrokken vanuit het lijn management van DPC. Pas bij het bedenken van passende maatregelen vanaf 8 januari wordt de plv. CIO betrokken bij de afhandeling van het incident;

[4] Voorschrift Informatiebeveiliging Rijksdienst
[5] Baseline Informatiebeveiliging Rijksdienst

- Het management van DPC heeft zich niet gerealiseerd welke risico's met deze opzet (systeem en werkproces) van de Mediabank werden gelopen en had in eerste instantie ook niet in de gaten dat het een probleem bij het Beeldcentrum betrof;
- Binnen het Beeldcentrum en ten aanzien van de werkzaamheden van het Beeldcentrum bij het management van DPC zijn geen mandateringsafspraken gemaakt;
- Het management van DPC veronderstelt dat de gebruikelijke werkwijze (het vroegtijdig voorbereiden achter de schermen) bij het, in opdracht van CKH, maken van een (standaard) video is, dat de afdeling CKH de video nog controleert. Dit is zelfs de hoofdreden om deze werkwijze te hanteren. Dat gebeurt in dit geval bij aanlevering door de NOS niet, omdat naar de mening van het management van de RVD een inhoudelijke check van video's aangeleverd door de NOS niet nodig is omdat de pDG aanwezig is geweest bij de opname;
- De benodigde kennis met betrekking tot de werkprocessen is bij de verschillende lagen van het management van DPC niet (altijd) adequaat;
- Het eerste aanbestedingscontract van de Mediabank is opgesteld door het toenmalige project onder aansturing van een Stuurgroep. Er was indertijd sprake van verschil in opvatting tussen de toenmalige CIO en de projectleider. Volgens zeggen ging dit verschil niet over beveiliging. Het tweede aanbestedingsdocument is eveneens opgesteld door het project en nagenoeg gelijk aan het eerste contract en is na overdracht door het project ondertekend door de pDPC. Evaluatie en leerervaringen zijn er niet geweest met betrekking tot de kwaliteitsverbetering van het eerste contract;
- In dit hele traject is er geen betrokkenheid geweest van de (plv.) CIO;
- Afdeling Beeldcentrum kent geen contract- of leveranciers management en kent geen structureel overleg met de leveranciers (Parkpost en Datiq) om de performance van hun diensten te bespreken;
- Afdeling Beeldcentrum is een jonge organisatie (gestart in januari 2011) ontstaan uit diverse teams van AZ (per 1 januari 2011) en BZK (per 1januari 2012). De professionaliteit en kwaliteit van deze teams liet naar zeggen te wensen over (contracten, mensen, financiën). De medewerkers zijn wel enthousiast, loyaal en gemotiveerd;
- Afdeling Beeldcentrum bestaat uit 13 fte en 2 uitzendkrachten. 2 medewerkers hebben ICT-kennis, maar slechts één heeft kennis van het informatiesysteem "Mediabank", maar is geen beveiligingsspecialist;
- Focus van het management van DPC ligt vooral op het beheersen van de huidige (crisis)situatie en nog niet op de structurele verbeteringen;
- Het management van DPC is onvoldoende op de hoogte van de inhoud van het contract met Parkpost en Datiq. De precieze taken van de hoofdaannemer Parkpost zijn niet bekend;
- Tot op heden was er geen reden om diepgaand naar de werkzaamheden van het Beeldcentrum te kijken. ICT was iets voor de specialisten ("zij zijn zelfredzaam");
- Het management van DPC heeft nooit expliciet over informatiebeveiliging ten aanzien van het Beeldcentrum gesproken. Men ging er van uit dat het publiektoegankelijke informatie betrof met een laag risicoprofiel. De aandacht lag sterk op andere onderdelen van DPC, zoals Rijksoverheid.nl;

- De afdeling Online Advies heeft haar informatiesystemen en de werkzaamheden daaromheen, in tegenstelling tot het Beeldcentrum, professioneler (VIR, Webrichtlijnen, Beveiliging, "productieknop", betrokkenheid (plv.) CIO, etc, etc.) georganiseerd. Het management van DPC heeft de professionaliteit van het Beeldcentrum niet op het niveau van Online Advies weten te brengen. Het management van DPC is wel bekend met VIR, etc.;
- De Manager C&M is zich er niet van bewust dat afdeling Beeldcentrum niet werkt conform de VIR, BIR.

De Mediabank

- De Mediabank is een systeem dat ontwikkeld is vanuit een project dat is overgegaan in de afdeling Beeldcentrum. De hosting is voor een tweede maal aanbesteed en (opnieuw) gegund aan Datiq (de laatste keer in combinatie met Parkpost);
- Men wil de Mediabank eind 2013 opnieuw aanbesteden. Doordat er plannen zijn om de Mediabank Rijksbreed in te zetten en een integratie met het platform van Rijksoverheid.nl overwogen wordt, is er een noodzaak om eerder dan in 2016 tot een nieuwe aanbesteding van de Mediabank te komen;
- Er zijn ideeën om vanwege de wens voor open source software en de kwetsbaarheid met betrekking tot de kennis over het huidige systeem om de Mediabank te integreren in het platform van Rijksoverheid.nl. Ook vanuit een oogpunt van beveiliging zou dat wenselijk zijn, maar dit werd niet als argument gehanteerd vóór het incident;
- Er wordt een second opinion uitgevoerd om de ideeën over integratie van de Mediabank in het platform van Rijksoverheid.nl te toetsen (al opgestart voorafgaand aan het incident);
- Bij de ontwikkeling rondom de Mediabank in de nabije toekomst spelen aspecten als de tijdelijke en structurele maatregelen en de integratie met het platform van Rijksoverheid.nl een rol.

Datiq (leverancier van hosting)

- Het lopende contract met Parkpost/Datiq is van kracht vanaf 1 augustus 2011 voor een periode van 2 jaar en de mogelijkheid om 3 keer te verlengen met een periode van 1 jaar. Strikt genomen moet vóór 1 augustus 2016 de Mediabank opnieuw aanbesteed worden. Uitbreiding van het gebruik van de Mediabank Rijksbreed in de nabije toekomst vereist echter een nieuwe aanbesteding;
- Bij Datiq was geen besef over hun eigen kwetsbaarheid vanwege het ontbreken van VOG's en geheimhoudingsverklaringen. Medewerkers van Datiq zijn volledig op de hoogte van de werking van het systeem. Het besef van dit potentiële risico element is afwezig;
- Het management van DPC acht Datiq een kundige en behulpzame organisatie, welke volgens het management van DPC de risico's, welke werden gelopen, ook niet heeft gezien;
- Datiq heeft sinds 24 december een zuivere opdrachtnemersrol vervuld, waarvan overigens ook al vóór het incident sprake was. Er is geen sprake van een gedefinieerde taakverdeling, aangezien iedereen lijkt te weten waar de eigen werkzaamheden stoppen en die van de andere partij beginnen.

Maatregelen[6] (tijdelijk en structureel)

- Direct na het incident zijn een aantal maatregelen uitgevoerd;
- In de eerste week van januari is volgend op de eerste selectieronde in de kerstnacht een aanvullende selectie uitgevoerd op semi-publieke (intranet) video's in het totale video-archief (2007-2012). Deze video's worden op een andere server geplaatst;
- Op 8 januari is een lijst met tijdelijke en structurele maatregelen opgesteld, welke op 9 januari door het MT besproken is. Hierbij heeft de directie de hoogste prioriteit gegeven aan het onbenaderbaar maken van intranetvideo's. De eerder aan Datiq gebriefde en de in de notitie van 8 januari opgesomde maatregelen kregen daarmee min of meer automatisch een lagere prioritering;
- De beschreven tijdelijke maatregelen lijken effectief, maar zijn suboptimaal en niet structureel bruikbaar;
- De maatregelen komen van de betrokken afdeling en zijn met medewerkers van de afdeling Online Advies, van Datiq en met de CIO en het MT besproken;
- Reeds nu blijkt dat de implementatie van de maatregelen meer tijd vergt dan voorzien;
- Omdat men bij het Beeldcentrum overweegt om met de Mediabank naar een ander platform te migreren (open source software) eind 2013, is er feitelijk geen sprake van structurele maatregelen. Als tijdelijke maatregelen worden die maatregelen beschouwd die voor 31 januari geëffectueerd zijn. Zie tabel in bijlage: 1, 2, 3, 9, 10, 14, 15, 16, 17, 18, 19. Over de overige maatregelen is nog geen besluit genomen;
- De tijdelijk genomen maatregelen zijn effectief voor de korte termijn, echter niet op lange termijn (bijvoorbeeld naamgeving in relatie tot de webrichtlijnen);

[6] Om veiligheidsredenen zijn enkele passages over concrete maatregelen en de tabel in de bijlage weggelaten en apart aangeboden.

- Het registreren van IP-adressen die toegang moeten hebben, middels gebruikmaken van een Whitelist (ACL[7]), betekent een extra beheerinspanning en het vergroten van kans op fouten wat het doorlopen van het workflowproces door gebruikers kan beïnvloeden (geen toegang tot bestanden hebben). Het is dus een suboptimale oplossing voor beveiliging van het systeem;
- Volgens Fox-IT hebben de overige maatregelen geen effect op het voorkomen van genoemd incident. De voorgestelde maatregelen behelzen niet het rigoureus beveiligen van de omgeving met bijvoorbeeld een DMZ;
- Een aantal maatregelen draagt overigens niet bij aan het voorkomen van een incident zoals zich heeft voorgedaan, maar dit levert wel een verbetering van de beveiliging van het gehele systeem op.

Juridische aspecten

Een eerste juridische analyse geeft als uitkomst dat Roeleveld geen strafbaar feit heeft gepleegd, noch bij het vinden van de kersttoespraak, noch bij het plaatsen van de link op Twitter, zodat de kersttoespraak openbaar werd. Van belang hierbij is dat de video van de kersttoespraak niet classificeert als "Staatsgeheim". Een strafvervolging lijkt weinig kans van slagen te hebben, nog afgezien van het publicitaire aspect (overheid vervolgt de klokkenluider).

Conclusies

Ten aanzien van het vaststellen waar procedures en/of menselijke fouten of nalatigheden hebben gefaald kan geconcludeerd worden dat er feitelijk geen sprake is van een menselijke fout of nalatigheid die in directe zin heeft geleid heeft tot dit incident.
Wel is er sprake van nalatigheid wanneer het gaat om het ontwikkelen, implementeren en auditten van de beveiliging van het systeem, de werkwijze en de in dit kader functionerende betrokken interne en externe medewerkers.
De medewerkers van deze jonge afdeling van DPC werken met veel inzet, enthousiasme en motivatie aan de taken die hen zijn opgedragen. De wisselwerking tussen hun kennis en die van de plv. CIO, de collega's van Online Advies en van de externe leverancier en de resultaten van mogelijk onafhankelijk uitgevoerde audits had moeten plaatsvinden en had daardoor het management van DPC er toe moeten zetten te komen met corrigerende en aanvullende maatregelen. Naast het MT van DPC had het initiatief hiertoe ook verwacht mogen worden van de leverancier en/of de specialisten.

Gebleken is het tekort schieten van veiligheidsbewustzijn van alle directe en indirecte betrokkenen bij het Beeldcentrum van DPC.

Ten aanzien van de maatregelen die tot dusver zijn getroffen om herhaling of een

[7] Een Access Control List (ACL) is een tabel met regels die de rechten (permissions) bepalen. Deze regels hebben betrekking op de toegang die gebruikers hebben tot bepaalde systeemobjecten of netwerkomgevingen. Access control lists worden doorgaans toegepast op bestandstructuren (bestanden/ mappen) of netwerkstructuren (poortnummers/ ip adressen).

vergelijkbaar incident te voorkomen kan geconcludeerd worden dat de tijdelijke maatregelen effectief zijn, maar suboptimaal en veel menselijk handelen vergen en daarmee ook de mogelijkheid op nieuwe fouten binnen de workflow.
De tijdelijke maatregelen zijn niet geschikt om te dienen als structurele maatregelen. Het management van DPC moet nu focussen op een stabiele veilige omgeving. Op dit moment vindt er een discussie plaats over een nieuwe aanbesteding, het gebruik van open source software en van integreren van de Mediabank in de omgeving van Rijksoverheid.nl.
Het management van DPC moet zich focussen op de beveiliging van de Mediabank, op verdere implementatie van de tijdelijke maatregelen, uitvoeren van de betrokken richtlijnen en het strikter uitvoeren van contract management. Met het oog daarop moet desnoods een verlenging van het contract met Parkpost/Datiq worden aangegaan (het contract met Parkpost/Datiq biedt hiertoe ruimte), zodat de nodige tijd genomen wordt om onderzoek te doen naar de integratie van de systemen. Op zich naar ons oordeel een logische gedachte. Er ontstaat echter een verhoogd risico wanneer in een te korte tijd te veel wijzigingen ondoordacht worden ingevoerd.

Aanbevelingen

1. Onderzoek en ontwerp op korte termijn een beveiligde architectuur voor de huidge Mediabank. Doe dit met medewerkers van het Beeldcentrum, afdeling Online Advies, plv. CIO, Datiq en een deskundige externe partij. Denk bij die architectuur in OTAP (ontwikkel-, test-, acceptatie-, productieomgeving) en DMZ structuren, in combinatie met een secured server. Laat daarna een second opinion uitvoeren op het resultaat van dit onderzoek en ontwerp.

2. Geef voorrang aan de uitvoering van de implementatie van deze nieuwe architectuur, boven het geforceerd snel overgaan op open source software en/of integreren met de omgeving van Rijksoverheid.nl. Overweeg om het hostingscontract met Parkpost/Datiq met 1 jaar te verlengen, onder verhoogde beveiligingsconditie en daarmee niet de aandacht te focussen op het proces van een nieuwe aanbesteding met allerlei nieuwe specificaties.

3. Zorg met spoed dat er gewerkt wordt en systemen en toepassingen ingericht worden conform de VIR, BIR en Webrichtlijnen. Regel acuut beveiligingsissues met de leveranciers (VOG en geheimhoudingsverklaring van externe medewerkers). Regel met spoed een jaarlijks terugkerende security audit.

4. Met het oog op doorgroei van de Mediabank voor Rijksbreed gebruik is het wenselijk dat de nodige tijd genomen wordt om onderzoek te doen naar de integratie en eventuele implementatie van de systemen (Mediabank en Rijksoverheid.nl).

5. Zorg dat de ICT-kennis binnen de afdeling Beeldcentrum verbreed wordt, bijvoorbeeld door een striktere samenwerking en/of collegiale toetsing door de afdeling Online Advies.

6. Zorg op korte termijn voor een structurele betrokkenheid van de CIO bij alle ICT-gerelateerde zaken binnen DPC en AZ breed en organiseer een leveranciersoverleg waarbij security als agendapunt genoteerd staat.

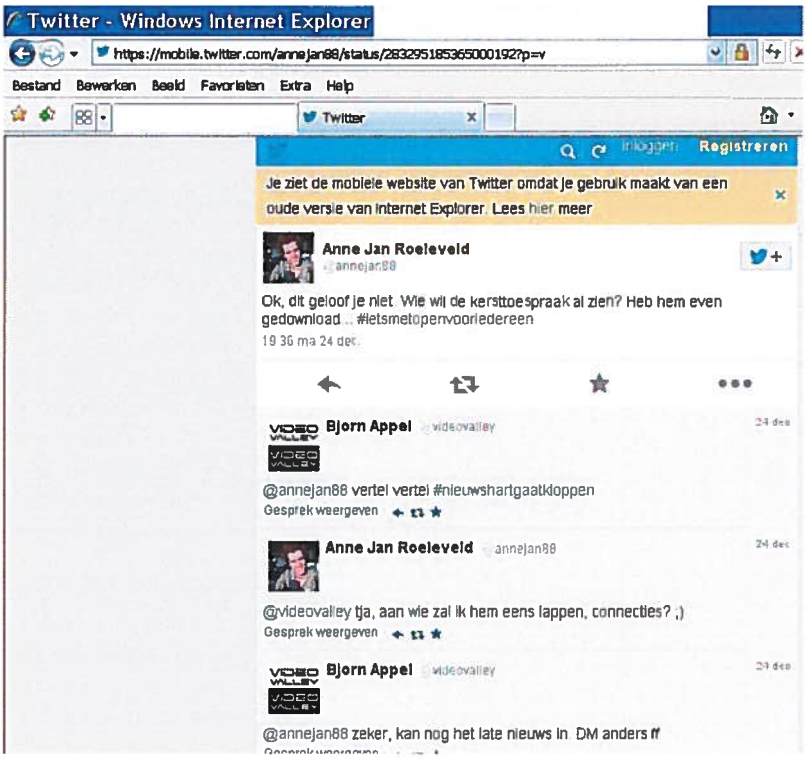
7. Waar nodig betere vastlegging van procedures en protocollen.

8. Meer in algemene zin is het van belang dat onder leiding van de CIO een visie op een beveiligingsarchitectuur wordt ontwikkeld voor het departement.

9. Borg dat in alle lagen van het management van DPC, bij de (plv.) CIO en bij de medewerkers van DPC het veiligheidsbewust zijn aanwezig is.

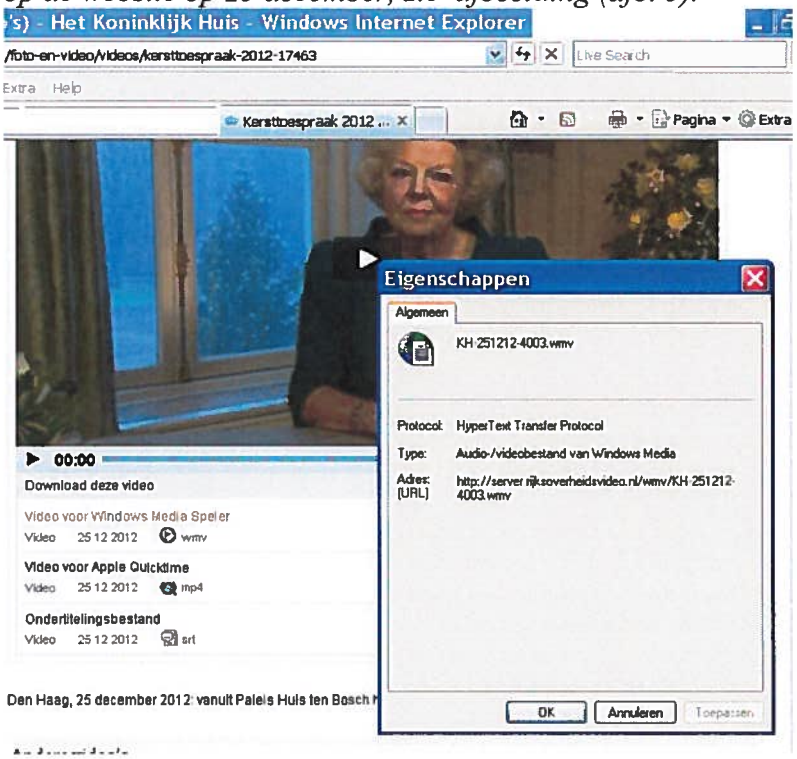
Bijlage – Afbeeldingen en tabel

Afb. 1: Informatie over het tijdstip van het moment waarop Roeleveld zijn eerste tweet verzond: 19:36 ma 24 dec

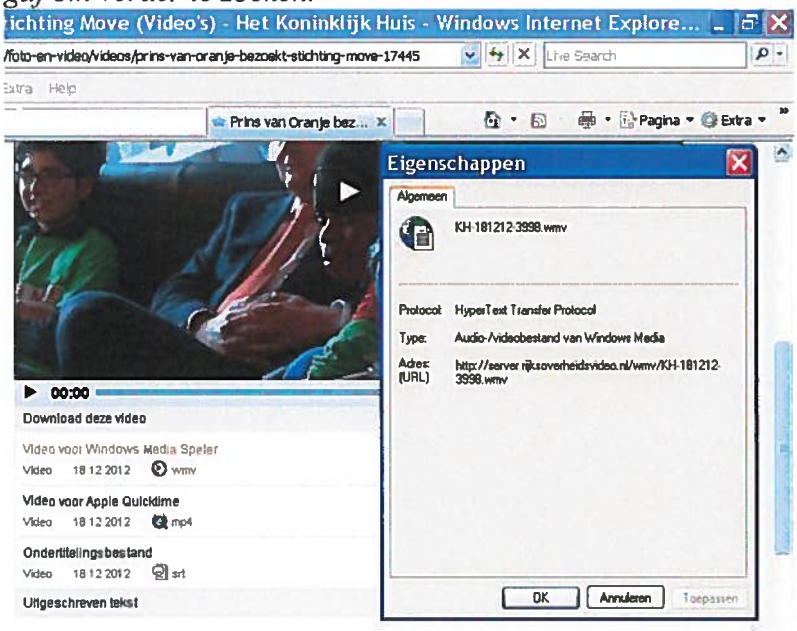


Afb. 2: 4 tweets verder, de "BREAKING" tweet.

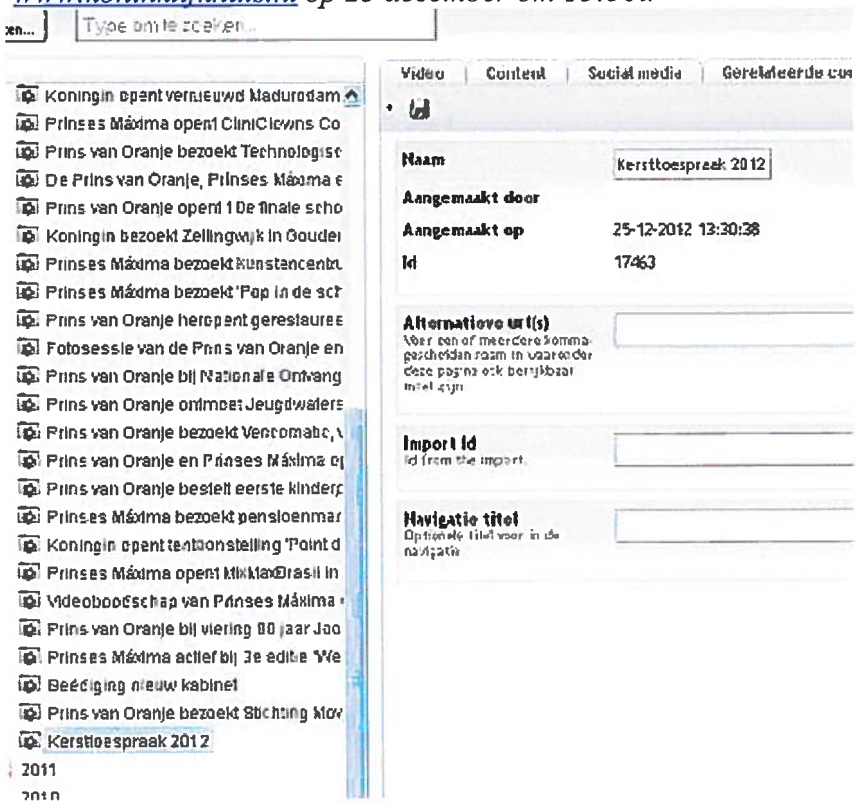
Afb. 3: Het bewuste adres (URL) van de video van de kersttoespraak van H.M. de Koningin. Deze informatie is ook terug te vinden in de broncode van de webpagina: file: 'http://server.rijksoverheidsvideo.nl/high/KH-251212-4003_hd.mp4'
NB: deze informatie, zoals hier afgebeeld, is pas te vinden na plaatsen van deze informatie op de website op 25 december, zie afbeelding (afb. 5).



Afb. 4: Het adres (URL) van een eerdere reeds geplaatste video die mogelijk aanleiding gaf om verder te zoeken.



Afb. 5: Schermafdruk van het publiceren van de kersttoespraak op www.koninklijkhuis.nl op 25 december om 13:30u



Afb. 6: Volgens de logging van het systeem het moment van de HIT, gevonden binnen 3 minuten:

Gebruiker ("hacker") haalt eerst files op (de player doet dat) die zijn gepubliceerd op:

http://www.koninklijkhuis.nl/foto-en-video/videos/kersttoespraak-2011-15617

http://server.rijksoverheidsvideo.nl/crossdomain.xml
http://server.rijksoverheidsvideo.nl/ondertiteling/KH-251211-2960.srt
http://server.rijksoverheidsvideo.nl/foto/KH-251211-2960.jpg
http://server.rijksoverheidsvideo.nl/high/KH-251211-2960_hd.mp4

Vervolgens probeert gebruiker:

24/Dec/2012:20:33:18 http://server.rijksoverheidsvideo.nl/high/KH-251211-2960_hd.mp4 (lukt)
24/Dec/2012:20:33:25 http://server.rijksoverheidsvideo.nl/high/KH-251212-2960_hd.mp4 (404 error)
24/Dec/2012:20:33:29 http://server.rijksoverheidsvideo.nl/high/KH-251212-2961_hd.mp4 (404 error)
24/Dec/2012:20:33:33 http://server.rijksoverheidsvideo.nl/high/KH-251212-2962_hd.mp4 (404 error)

(7 seconden later, n.a.v. van bezoek http://www.koninklijkhuis.nl/foto-en-video/videos/prins-van-oranje-bezoekt-stichting-move-17445)

24/Dec/2012:20:33:40 http://server.rijksoverheidsvideo.nl/ondertiteling/KH-181212-3998.srt (referral: http://www.koninklijkhuis.nl/foto-en-video/vide
van-oranje-bezoekt-stichting-move-17445)
24/Dec/2012:20:33:40 http://server.rijksoverheidsvideo.nl/foto/KH-181212-3998.jpg (referral: idem)

(13 seconden later, geen referral, maar directe URL intypen dus)

24/Dec/2012:20:34:53 http://server.rijksoverheidsvideo.nl/high/KH-191212-3998_hd.mp4 (404)
24/Dec/2012:20:34:58 http://server.rijksoverheidsvideo.nl/high/KH-181212-3998_hd.mp4 (bestaat, prins en stichting MOVE)
24/Dec/2012:20:35:13 http://server.rijksoverheidsvideo.nl/high/KH-251212-3999_hd.mp4 (404)
24/Dec/2012:20:35:17 http://server.rijksoverheidsvideo.nl/high/KH-251212-4000_hd.mp4 (404)
24/Dec/2012:20:35:20 http://server.rijksoverheidsvideo.nl/high/KH-251212-4001_hd.mp4 (404)
24/Dec/2012:20:35:23 http://server.rijksoverheidsvideo.nl/high/KH-251212-4002_hd.mp4 (404)
24/Dec/2012:20:35:26 http://server.rijksoverheidsvideo.nl/high/KH-251212-4003_hd.mp4 (HIT)