Kort verslag Ruby on Rails calamiteit DigiD 9-1-2013

Intern werkdocument Logius

Chronologie
In de vroege ochtend van 9 januari 2013[1] meldt een van de bij DigiD betrokken leveranciers van DigiD dat de community van gebruikers van de onderliggende software Ruby on Rails waarvan deze leverancier actief lid is (1) een ernstige kwetsbaarheid heeft ontdekt en (2) later die ochtend een oplossing beschikbaar zal komen in de vorm van een patch om de kwetsbaarheid op te heffen. Ruby on Rails is een open source softwareframework om webapplicaties mee te programmeren. Naast DigiD gebruiken vele honderden bedrijven dit framework, waar onder Groupon, Twitter en Soundcloud. De leverancier van DigiD adviseert zo snel mogelijk te acteren.

Logius schakelt onmiddellijk het NCSC in om te helpen bij het maken van de afweging wat te doen. Na analyse bevestigt het NCSC later die ochtend telefonisch dat het inderdaad om een ernstige kwetsbaarheid gaat. Tevens bevestigt het NCSC dat er van moet worden uitgegaan dat het op zeer korte termijn – vermoedelijk binnen een dag - mogelijk wordt misbruik te maken van de kwetsbaarheid.

Mede op basis van dan inmiddels door Logius zelf gedane verdere analyses concludeert Logius op dat moment als volgt:

- De kwetsbaarheid moet zo snel mogelijk worden verholpen. Zodra kwaadwillenden in staat zijn de kwetsbaarheid te misbruiken, leidt dat er toe dat de databases achter een website geraadpleegd kunnen worden. Dat zou kunnen betekenen dat een kwaadwillende alle in DigiD opgeslagen gegevens kan raadplegen, zoals naam en burgerservicenummer. Hij of zij moet dan overigens nog steeds meer weten van het ontwerp van DigiD om daadwerkelijk gegevens te kunnen raadplegen. Deze kennis is niet publiekelijk beschikbaar.
- Er is vooralsnog geen enkele aanwijzing dat het inmiddels ook daadwerkelijk iemand gelukt is om de betreffende kwetsbaarheid te benutten, laat staan DigiD te misbruiken.
- Voordat de patch in productie gaat moet deze zorgvuldig zijn getest – zowel functioneel als op het gebied van beveiliging. De installatie en het uitvoeren van alle tests volgens de procedures kent een doorlooptijd van ongeveer 12 uur.

De vraag is wat te doen. Voor Logius staat de betrouwbaarheid van DigiD voorop: liever een tijdelijk niet beschikbaar systeem dan een systeem dat niet meer vertrouwd kan worden. De opties zijn:

1. DigiD blijft draaien met als risico dat de kwetsbaarheid ondertussen misbruikt wordt. Voordeel is onverstoorde dienstverlening en blijvende beschikbaarheid van DigiD. Nadeel is dat DigiD getroffen kan worden. De kans op misbruik wordt gering ingeschat, de impact enorm met als ernstigste variant de mogelijkheid dat alle ruim 10 miljoen DigiD accounts vervangen moeten worden.
2. DigiD wordt preventief uit de lucht gehaald. Dit betekent dat burgers en publieke dienstverleners enige tijd geen zaken met elkaar kunnen doen waarbij DigiD nodig is. DigiD uit de lucht halen leidt tot veel media-aandacht en communicatie met klanten en burgers. Het voordeel is dat geen misbruik gemaakt kan worden van de kwetsbaarheid.

Om 11 uur kiest Logius definitief voor de tweede optie: DigiD wordt preventief uit de lucht gehaald, omdat de risico's onverantwoord groot zijn. Dit besluit wordt kort daarop geëffectueerd:

1. DigiD wordt preventief uit de lucht gehaald
2. De klanten, de beleidsopdrachtgevende directie van BZK, de ambtelijke top en de Minister van BZK worden op de hoogte gesteld.
3. Bij het aangeven van de te verwachten oplostijd wordt enige marge in acht genomen met het oog op mogelijke problemen
4. Op de website van DigiD wordt vermeld dat DigiD vanwege een geconstateerde kwetsbaarheid per direct preventief uit de lucht is gehaald en naar verwachting de

[1] In Bijlage 1 is het interne Logius logboek weergegeven van de gebeurtenissen op deze dag

volgende ochtend weer beschikbaar zal zijn.
5. De patch wordt conform het voor dit soort situaties gehanteerde standaard proces geïnstalleerd, getest in de testomgeving en daarna in productie genomen.

Het besluit leidt direct tot veel media aandacht. Nog voordat Logius in staat is geweest zelf alle klanten, de beleidsopdrachtgevende directie van BZK, de ambtelijke top en de Minister toelichting te geven melden de media al dat DigiD uit de lucht is.

Het in productie nemen van de patch en daarmee de oplossing van het probleem en het weer in de lucht brengen van DigiD verlopen verder voorspoedig en conform plan. Eerder dan in de interne tijdplanning voorzien is DigiD 's avonds weer voor gebruik beschikbaar.

Leerpunten en bemerkingen

1. In de latere media aandacht is hier en daar opgemerkt dat dit soort kwetsbaarheden voorkomen kunnen worden en dat het gebeurde aantoont dat DigiD onveilig is. De visie van Logius is dat op zichzelf elke kwetsbaarheid er een te veel is, maar de realiteit – ook bij Logius - is dat elke softwareomgeving kwetsbaarheden kent. De cruciale vraag die Logius zichzelf naar aanleiding van het gebeurde primair heeft gesteld is, of Logius meer had kunnen/moeten doen dan is gedaan. Uit de zelfevaluatie is geconcludeerd dat, los van kleine verbeterpunten, adequaat is gehandeld en dat het herstelvermogen van de organisatie bij deze gebeurtenis goed is gebleken.
2. Ook is hier en daar de discussie ontstaan of Logius terecht gebruik maakt van open source software. Logius hanteert de enkele jaren geleden, mede op uitdrukkelijk verzoek van de Tweede Kamer door het kabinet vastgestelde algemene beleidslijn open source te zien als volwaardig alternatief voor closed source producten. Logius heeft in het gebeurde voorts geen aanleiding gevonden om thans de keuze te heroverwegen voor gebruik van het in dit specifieke geval kwetsbaar gebleken specifieke open source softwareframework Ruby on Rails. De actieve participatie in de Ruby on Rails community van een van de bij DigiD betrokken leveranciers van DigiD borgt naar het oordeel van Logius in voldoende mate dat kwetsbaarheden tijdig bij Logius bekend zijn en weggenomen kunnen worden. Dit tegen de achtergrond van de vergelijking van de mogelijkheden tot borging indien andere keuzen zouden zijn of worden gemaakt.
3. Logius heeft na het gebeurde uitgebreid onderzoek gedaan om te bepalen of de kwetsbaarheid heeft geleid tot verlies van en/of onbevoegde inzage in data of vertrouwelijke informatie. In overleg met de betrokken leverancier is een reguliere root analyse een diepgaande extra analyse gedaan. Uit de logging blijkt dat zich geen onregelmatigheden hebben voorgedaan en de belangrijkste queries niet geraakt zijn. Geconcludeerd is dat niets wijst op een succesvolle informatielek of inbraak op de accounts database, het meest gevoelige deel.

Bijlage: logboek 9-1-2013

07:52: Een van de bij DigiD betrokken leveranciers meldt Logius een Ruby On Rails probleem per e-mail. In deze email wordt niet duidelijk vermeld wat het probleem is, er wordt alleen aangeven dat er probleem is en dat gewerkt wordt aan een patch voor DigiD.

08:50 Na enkele contacten trekt de deskundigen van Logius de conclusie dat er sprake is van een zeer ernstige kwetsbaarheid in Ruby on Rails, dat DigiD potentieel met automatische tooling eenvoudig te hacken zou zijn en dat voorbereidingen gestart zouden moeten worden om DigiD offline te brengen. De leverancier zal zijn advies per mail bevestigen.

09:00 De calamiteitmanager van Logius is geïnformeerd en deze informeert op zijn beurt de Logius directie. Besloten wordt het NSCS advies te vragen en ondertussen de voorbereidingen voor het offline brengen van DigiD af te ronden.

09:45 NCSC bevestigt de ernst van de situatie en de – grote - kans dat later die dag de mogelijkheid er zal zijn daadwerkelijk gebruik te maken van de kwetsbaarheid.

10:00 Het calamiteitenteam bespreekt de scenario's.

11:30 De leverancier meldt dat de patch definitief gereed is voor DigiD die de gevonden problematiek oplost en de kwetsbaarheid doet verdwijnen. De Logius directie heeft inmiddels besloten DigiD offline te brengen en tegelijkertijd tests uit te laten voeren op de ACC2 omgeving van DigiD met de nieuwe patch. Het calamiteiten team heeft besloten om een regressie test uit te voeren en om een security test uit te laten voeren.

12:00 DigiD is offline gebracht. De testers zijn gebeld dat zij om 18:00 kunnen starten met de security test.

13:00 DigiD (met patch) is uitgerold op de ACC2. De testers starten direct met de regressietest en verwachten de automatisch regressietest om 17:00 af te ronden. Daarna zal Logius aan testers de opdracht geven om te starten met de security test om te bevestigen dat het lek is opgelost. Daarna zal ook de preproductie1 van DigiD worden voorzien van de nieuwe versie (incl patch). De leverancier heeft van Logius de opdracht gekregen om ook de preproductie1 omgeving van DigiD te voorzien van een patch.

13:30 Belastingdienst is ingelicht en gevraagd om standby te staan voor een hertest van DigiD (met patch op preproductie1). Zij hebben aangegeven dat dit kan tot 16:30.

15:00 Belastingdienst heeft een hertest uitgevoerd op de preprod1. DigiD met security patch. Belastingdienst heeft heeft akkoord gegeven.

16:44 De regressie test is succesvol afgerond. Er zijn geen bevindingen in naar boven gekomen. De test van de Koppelvlakken en de Beheermodule moeten nog worden afgerond.

17:45 De regressie volledig afgerond.

18:08 De testers starten de security test

20:30 De testers rapporteren dat de security test geslaagd is. De bevestiging komt eraan.

21:00 De testers bevestigen dat de security test op de ACC2 omgeving uitwijst dat DigiD niet meer kwetsbaar is! Het advies is weer live te gaan.

21:01 Logius en haar leverancier beginnen met de uitrol van DigiD (met patch) naar de productie omgeving. Na verwachting staat het voor 22:00 live.

21:30 Logius geeft akkoord voor het vrijgeven van DigiD. De beheermodule en burger applicatie zijn gecontroleerd en akkoord bevonden.

22:00 DigiD is live.