**Risico en Beveiligingsanalyse**

**Vooraf**

De opsplitsing van het Vooronderzoek in Definitie, Haalbaarheid, Systeem analyse is gebaseerd op stappen uit de “Information System Development Life Cycle” (ISDLC). Het Risicomanagement heeft daarin het doel om de risico’s vast te stellen en om zich voor te bereiden op de veroorzakende factoren. Uiteindelijk moet dan de vraag beantwoord worden of een systeem moet worden vervangen. De uitkomst van dit proces is echter al bekend. Er moet een Promo Delivery System worden ontworpen.

In deze analyse zal inzichtelijk worden gemaakt welke dreigingen voor het nieuwe systeem relevant zijn, wat de risico’s zijn en welke maatregelen kunnen worden genomen. Belangrijk hierbij is dat de maatregelen zich richten op het hele ontwikkel proces en in alle fases van de ontwikkeling moeten worden toegepast.

**Context**

De opdrachtgever is Hexagon, een Fanclub organisatie van DJ Don Diablo. Dit project gaat over de ontwikkeling voor een systeem waarin fans, die zelf ook vaak muziek maken, demo’s kunnen inzenden ter beoordeling.

Er is op dit moment al een mogelijkheid om via een fan-website demo’s in te sturen. De huidige werking van het systeem is dat er via een standaard HTML formulier op de Website van Hexagon een aantal gegevens worden ingevuld. De Web server wordt gehost door squarespace.com via een veilige SSL verbinding. Het Demo bestand wordt samen met de gegevens gemaild naar de backoffice van Don Diablo aan promo@dondiablo.com Het Promo systeem wat moet worden opgeleverd zal Audio samples van fans/producers en reacties van het Hexagon team bevatten.

Gevraagd is een web toepassing om de beoordeling van de demo’s binnen Hexogon eenvoudiger af te handelen.

Het wordt een gesloten systeem waar alleen de fans die zich hebben aangemeld en het Hexagon Team toegang toe zullen krijgen. Binnen het systeem zijn meerde gebruikers rollen. De ***fans*** kunnen alleen demo’s insturen. De ***medewerkers*** van Hexagon kunnen demo’s afluisteren en een reactie toevoegen. De ***administrator*** kan gebruikers en demo bestanden wissen.

*Facts*

Er worden geen persoonlijke gegevens die onder de wet AVG vallen, opgeslagen in het systeem.

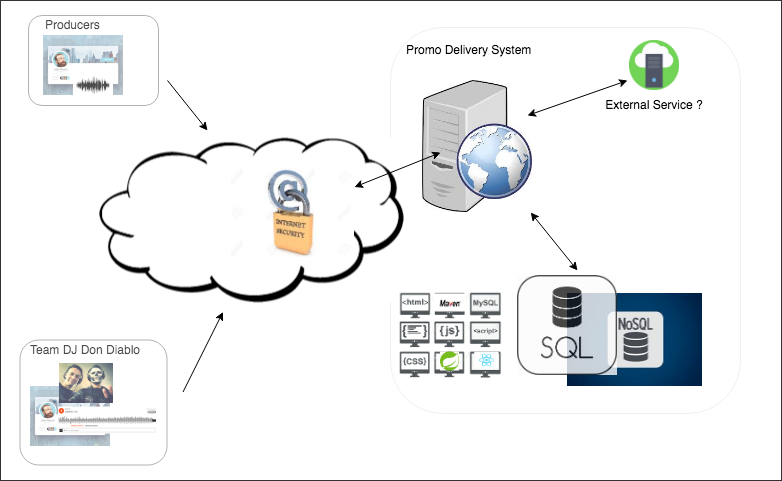
De demo’s worden ingezonden met het doel om openbaar gemaakt te worden en hoeven ook niet streng vertrouwelijk te worden behandeld.

Het Promo systeem zal niet worden geïntegreerd met de bestaande website maar in een aparte omgeving draaien met eigen data opslag

De beoordeling van de demo’s is vertrouwelijk en wordt liever niet openbaar gemaakt.

De passworden van de gebruikers zijn zeer vertrouwelijk en mogen in geen geval openbaar worden gemaakt.

DJ Don Diablo is een bekend persoon en daardoor kwetsbaar voor imagoschade



**Dreigingen en risico’s**

***Hacking van het systeem van buiten af met risico van:***

- Diefstal van gebruikersgegevens en demo bestanden

- Diefstal van gebruikers passwoorden

- Verlies/beschadiging/openbaar maken van gebruikers gegevens en beoordelingen

- Imago schade voor gebruikers en Hexagon

Omdat de applicatie beveiligd is bestaat er een verhoogd risico op inbraakpogingen omdat inlog gegevens van gebruikers waardevol zijn voor hackers. De kans dat hackers proberen in te breken is duidelijk aanwezig omdat de site via openbaar Internet is te bereiken en omdat DJ Don Diablo een bekende persoon is.

De omvang van de schade kan indirect hoog zijn als inlog gegevens van gebruikers kunnen worden misbruikt op andere websites. Het is voor DJ Don Diablo slechte reclame als via zijn Promo Site gegevens worden gelekt.

***Poging tot uitvoeren van ongeoorloofde handelingen door gebruikers met risico van:***

- Verlies/beschadiging/openbaar maken van gebruikers gegevens en beoordelingen

- Imago schade voor gebruikers en Hexagon

Gebruikers die toegang hebben tot het systeem kunnen altijd expres of per ongeluk acties proberen uit te voeren die niet zijn geoorloofd. Een hacker die toegang zoekt met slechte bedoelingen kan natuurlijk ook een account maken en vandaaruit proberen ongeoorloofde handelingen uit te voeren.

De omgang van de schade is beperkt omdat de gegevens niet bijzonder vertrouwelijk of waardevol zijn. Het herstellen van de gegevens kan eenvoudig mogelijk worden gemaakt door een betrouwbare hosting partner te kiezen. De reputatie schade is daarom ook minder ernstig.

***Uitval/Onbereikbaarheid van het systeem met risico van:***

- Onbereikbaarheid demo’s en boordelingen

- Imago schade voor Hexagon

De kans op uitval door storing of een ddos aanval is relatief laag. De applicatie zal extern worden gehost

De omgang van de schade is laag omdat een tijdelijke onbereikbaarheid van de gegevens niet ernstig is. Het herstellen van de toegang kan eenvoudig mogelijk worden gemaakt door een betrouwbare hosting partner te kiezen . De reputatie schade is daarom ook laag.

**Maatregelen**

Bij het ontwerp, ontwikkeling en het testen van de applicatie zal beveiliging steeds een aandachtspunt moeten zijn.

Concreet stappen die in de workflow van het project kunnen worden opgenomen zijn:

In de ontwerp fase :

* In User Stories ook de beveiliging en testen meenemen. *Bv. “Als Developer/Architect wil ik zeker weten EN als Security/Tester wil ik verifiëren dat het password van de gebruiker niet kan worden onderschept”*
* Gebruik maken van veilige en beproefde technologieën, frameworks en libraries als Spring Boot/Maven

*Dus geen eigen ‘slimme’ veiligheidsclasses proberen te bedenken of ‘zomaar’ een Library gebruiken.*

* Code opsplitsen in beveiligingsklassen. *Bv. scripts splitsen en alleen de voor de noodzakelijke blokken opnemen die nodig zijn voor het rol profiel van de gebruiker. En.. In de MVC architectuur Aparte Controllers maken voor iedere beveiligingsrol.*
* Op meerdere plaatsen in de code testen of de actie is toegestaan in het profiel van de gebruiker. *Bv. niet alleen bij de aanroep testen maar ook binnen de subroutines blijven controleren.*
* Maatregelen op basis van ‘attack patterns’ en bekende dreigingen toepassen. Microsoft STRIDE / OWASP top 10 / SANS top 20 *Bv. gevaar van SQL Injection kan in het ontwerp al worden uitgesloten.*
* Review laten doen van ontwerp door Ethical Hacker

In de ontwikkel fase:

* Security Unittesten schrijven.
* OWASP checklist toepassen
* Code review door ethical hacker

**Attack patterns en bekende dreigingen**

De bekende bedreigingen kunnen door hackers met tools geautomatiseerd worden gescand. Deze dreigingen zijn dus zeer reel en de kans op ontdekking is groot. De bekende dreigingen zijn goed gedocumenteerd en ook de maatregelen die genomen kunnen worden zijn bekend. In de ontwerp/ontwikkel en test fase moet in ieder geval de top 10 van OWASP worden afgedekt.

In de bijlage:

OWASP Application Security Verification Standard 4.0 (maart 2019)

OWASP Pro Active Controls v3.0 (2018)

2019 CWE Top 25 Most Dangerous Software Errors (2019)