Risicoanalyse (BCM Plan)

Intra Cloud

Projectgroep	Cloud 9	
Auteurs	Tim Spies	(578800)
	Michael Kalil	(590395)
	Daan Reynaert	(581389)
	Mark de Heus	(601498)
	Koen Bongers	(603274)
Opdrachtgever	Sander Maijers	

Datum	16-05-2020
Locatie	Arnhem
Semester	Verdiepend semester
Course	DIOS-P
Opdracht	HANubes

Inhoud

1. Inleiding

Uiteraard is de continuïteit van de dienstverlening van groot belang voor toekomstige afnemers. Niet voor niets is de vraag van 7x24 uur beschikbaarheid geformuleerd. Om hieraan bij te dragen is een risicoanalyse gemaakt. Deze is op basis gemaakt voor de toekomstige productieomgeving. Hierbij staan de voorgestelde maatregelen om de continuïteit van de dienstverlening te realiseren.

2. Risicoanalyse

In de businesscase is een risicobeoordeling uitgevoerd met de scope van het Proof of Concept. Deze risicoanalyse bevat echter de scope van de gehele toekomstige productieomgeving. Dezelfde risicobeoordeling matrix zal hierbij gebruikt worden. Hierbij staan een aantal kolommen zoals o.a. genaamd ‘score’, ‘kans’ en ‘impact’. De kans is een cijfer op schaal van 1 tot 10 waarbij 1 het te verwachten risico weergeeft en 10 heel onwaarschijnlijk is. Hetzelfde geldt voor de impact, alleen hierbij weergeeft het cijfer 10 een kritieke toestand voor het project. De kolom score weergeeft de algemene score van de risicobeoordeling voor een bepaalde risico. Deze score is bepaald aan de hand van de berekening *Score = Kans * Impact* (Bron: Werkveilig) en kan maximaal 100 zijn. Zo kan in één oogopslag bekeken worden wat de hogere risico’s zijn. Verder is per risico een nummer toegewezen om deze gemakkelijk in te delen in de tweede tabel. In deze tabel wordt per risico de maatregelen beschreven. Zo kunnen de risico’s afgedekt worden (Het inschatten van risico’s middels : Risico = Kans x Effect, 2016).

2.1 Risicobeoordeling

Score	Risico nr + naam	Beschrijving	Kans	Impact
3	R1- Geen internettoegang	Geen toegang tot het internet is beschikbaar voor de cloud ontwikkelaars.	3	1
6	R2- Verkeerde project doeleinden	De studenten gebruiken de cloudomgeving voor privé-projecten op commerciële basis.	6	1
16	R3- Stroomuitval	De stroom kan uitvallen waardoor de servers defect kunnen raken en de omgeving niet verder gebruikt kan worden.	2	8

9	R4- Hacker heeft toegang tot de cloud-omgeving	Een hacker heeft op een of andere manier toegang tot de cloud-omgeving gekregen waardoor hij een of meerdere servers kan exploiten/beschadigen.	1	9
24	R5- Studenten krijgen verkeerde rechten toegewezen	Studenten krijgen per ongeluk verkeerde rechten toegewezen door beheerders of docenten waardoor ze mogelijk onbevoegd toegang hebben.	4	6
25	R6- Onduidelijke oplevering	Bij de oplevering van het HANubes is niet genoeg duidelijkheid richting de HAN Beheerders waardoor de omgeving niet goed onderhouden kan worden.	5	5
20	R7- Te veel vragen vanuit gebruikers	Er is geen goede handleiding die het hele bereik van de aangeboden diensten dekt. Hierdoor zijn er veel vragen vanuit gebruikers.	4	5
8	R8- Invloeden vanuit buiten (natuurrampen)	Door een natuurramp gaat apparatuur kapot	1	8

24	R9- Kapotte apparatuur	Door onverwachte gebeurtenissen kan cruciale apparatuur kapot gaan die gebruikt wordt voor het project.	3	8
35	R10- Geen goede isolatie van applicaties	Doordat de opgeleverde services niet goed geïsoleerd zijn kunnen gebruikers van aparte omgevingen bij elkaar.	5	7
20	R11- Derdejaars ISM studenten maken misbruik van privileges	Derdejaars ISM studenten maken misbruik van privileges die ze gekregen hebben voor het beheer.	5	4
24	R12 - Foutieve configuratie door beheerder	Wanneer tijdens de ontwikkeling door beheerders een foutieve configuratie uitgevoerd wordt, ontstaat er een groot risico. Hierdoor kunnen bijvoorbeeld services uitvallen of gebruikers op verkeerd plekken terechtkomen.	4	4

Tabel 1 - Risicobeoordeling

Uit deze beoordeling blijkt dus dat het risico ‘Geen goede isolatie van applicaties’ het grootste risico met een score van 35 is voor de uiteindelijke realisatie van het project. Bij voorval van dit risico zal het ervoor zorgen dat gebruikers bij elkaars omgevingen kunnen. Hierdoor kan onbedoeld of bedoeld schade aangericht worden binnen projecten van andere gebruikers.

2.2 Maatregelen

Zoals eerder beschreven zullen in onderstaande tabel de maatregel(en) per risico benoemd worden, om ze zo af te dekken.

Risico nr + naam	Beschrijving	Omschrijving maatregel
R1- Geen internettoegang	Geen toegang tot het internet is beschikbaar	Omdat HANubes een private cloud gebaseerd project is heeft deze risico geen grote impact. Alle gebruikers werken lokaal op het HAN netwerk waarbij geen internet toegang naar buiten is. Alleen met grote uitzondering wordt een connectie met het internet gemaakt. Bijvoorbeeld wanneer bedrijven buiten de HAN gebruik maken van HANubes. Tot slot is een maatregel om de netwerkapparatuur redundant op te stellen.
R2- Verkeerde project doeleinden	De studenten gebruiken de cloud omgeving voor privé-projecten op commerciële basis.	Het is de taak van docenten om de omgevingen van studenten in de gaten te houden. Hierbij is het dus belangrijk dat docenten goed ingelicht worden op dit aspect.

R3- Stroomuitval	De stroom kan uitvallen waardoor de servers defect kunnen raken en de omgeving niet verder gebruikt kan worden.	Stroomtoevoer vanuit twee kanalen. Aanwezigheid van een noodaggregaat en noodstroomvoedingen (UPS).
R4- Hacker heeft toegang tot de cloud-omgeving	Een hacker heeft op een of andere manier toegang tot de cloud-omgeving gekregen waardoor hij een of meerdere servers kan exploiten/beschadigen.	Doordat HANubes intern gebaseerd is bestaat er een kleine kans dat een hacker toegang krijgt tot de omgeving. Het is belangrijk dat gebruikers op de hoogte zijn van de schade die hierbij kan opgewekt worden. Verder moeten de firewalls en routers/switches goed geconfigureerd zijn om deze kans te verkleinen.
R5- Studenten krijgen verkeerde rechten toegewezen	Studenten krijgen per ongeluk verkeerde rechten toegewezen door beheerders of docenten waardoor ze mogelijk onbevoegd toegang hebben.	Bij het ontwerpen van rechtenstructuur voor HANubes is hier goed over nagedacht. Het is zo geconfigureerd dat studenten beperkte rechten hebben en alleen hun eigen projecten kunnen aanpassen. Mocht het zijn dat een student meerdere rechten heeft door bijvoorbeeld een fout van een beheerder of docent kan dit opgevangen worden in het monitoringssysteem.
R6- Onduidelijke oplevering	Bij de oplevering van het HANubes is niet genoeg duidelijkheid richting de HAN Beheerders waardoor de omgeving niet goed onderhouden kan worden.	In de gehele toekomstige productieomgeving kan het zijn dat beheerders niet goed op de hoogte zijn van configuraties die in de PoC verwerkt zijn. Het is dus belangrijk dat de escalatie van PoC naar de volledige omgeving goed begeleid wordt door middel van handleidingen.

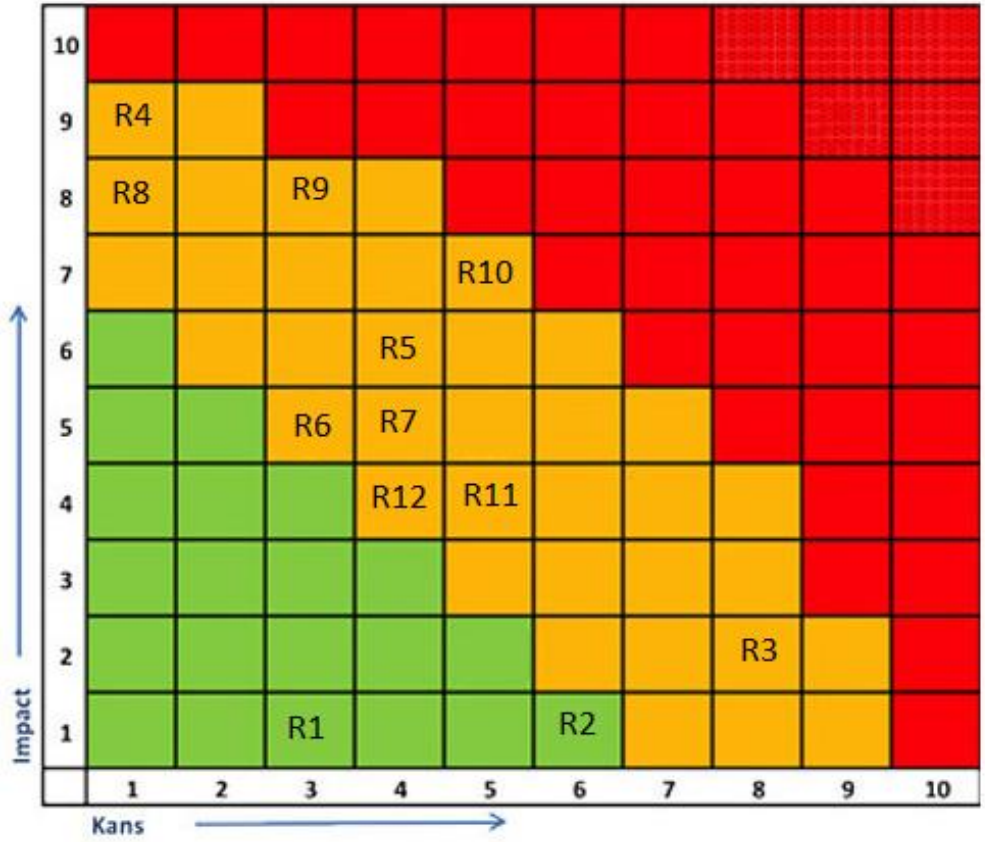
R7- Te veel vragen vanuit gebruikers	Er is geen goede handleiding die het hele bereik van de aangeboden diensten dekt. Hierdoor zijn er veel vragen vanuit gebruikers.	Dit risico heeft een koppeling met R6, door een onduidelijke oplevering van het PoC komen veel vragen vanuit gebruikers. Om dit te voorkomen is het belangrijk dat een goede handleiding geschreven wordt voor iedere doelgroep.
R8- Invloeden vanuit buiten (natuurrampen)	Door een natuurramp gaat apparatuur kapot	Dit risico is vanuit het HANubes project eigenlijk onmacht. Wel kunnen er maatregelen genomen worden zoals bijvoorbeeld hitte- en waterbestendige serverruimtes implementeren.
R9- Kapotte apparatuur	Door onverwachte gebeurtenissen kan cruciale apparatuur kapotgaan die gebruikt wordt voor het project.	Cruciale apparatuur die de kern van de cloudomgeving zijn moeten redundant opgesteld worden. Zo kan kapotte apparatuur overgenomen worden. Verder moeten wekelijkse back-ups minimaal incrementeel of full zijn. (incremental & full back-ups)
R10- Geen goede isolatie van applicaties	Doordat de opgeleverde services niet goed geïsoleerd zijn kunnen gebruikers van aparte omgevingen bij elkaar.	Webapplicaties isoleren.
R11- Derdejaars ISM studenten maken misbruik van privileges	Derdejaars ISM studenten maken misbruik van privileges die ze gekregen hebben voor het beheer.	Een student mag nooit een “top”-admin zijn in die hiërarchie.

R12 - Foutieve configuratie door beheerders	Wanneer tijdens de ontwikkeling door beheerders een foutieve configuratie uitgevoerd wordt, ontstaat er een groot risico. Hierdoor kunnen bijvoorbeeld services uitvallen of gebruikers op verkeerd plekken terechtkomen.	Beheerders moeten zich goed bewust zijn van de schade die zij kunnen richten door foutieve configuraties. Trainingen en workshops zijn daarvoor belangrijk. Het is gewenst om beheerders die met HANubes zullen werken de juiste hoeveelheid trainingen en workshops aan te bieden zodat zij minder fouten maken.

Tabel 1 - Risicomaatregelen

3. Conclusie & aanbevelingen

Om visueel duidelijk te krijgen waar de risico's van HANubes ingedeeld staan is hier een risicomatrix ontworpen met de Risico's erin (Figuur 1 - Risicomatrix HANubes). De risico's staan in de vorm van risiconummers beschreven (zoals in tabel 1 beschreven staat).



Figuur 1 - Risicomatrix HANubes

Zoals in de afbeelding beschreven staat zijn 3 risico's die zich aan de rode grens aansluiten. Voor deze 3 risico's zal hieronder een aanbeveling beschreven staan omdat deze het gevaarlijkst zijn.

- R4: Hacker heeft toegang tot de cloud-omgeving

Doordat HANubes intern gebaseerd is bestaat een kleine kans dat een hacker toegang krijgt tot de omgeving. Het is belangrijk dat gebruikers op de hoogte zijn van de schade die hierbij kan opgewekt worden. Verder moeten de firewalls en routers/switches goed geconfigureerd zijn om deze kans te verkleinen.

- R9: Kapotte apparatuur

Cruciale apparatuur die de kern van de cloudomgeving zijn moeten redundant opgesteld worden. Zo kan kapotte apparatuur overgenomen worden. Verder moeten wekelijkse back-ups minimaal incrementeel of full zijn. (incremental & full back-ups)

- R10: Geen goede isolatie van applicaties

Bij voorval van dit risico zal het ervoor zorgen dat gebruikers bij elkaars omgevingen kunnen. Hierdoor kan onbedoeld of bedoeld schade aangericht worden binnen projecten van andere gebruikers. Om dit te voorkomen is het een goed advies om bij het aanmaken van applicaties ervoor te zorgen dat gebruikers hun eigen poorten ingeven, waardoor portforwarding wordt ingeschakeld.

4. Bibliografie

Het inschatten van risico's middels : Risico = Kans x Effect. (2016, November 23). From werkveilig: https://werkveilig.wordpress.com/2017/11/23/gratis-het-inschatten-van-risicos-middels-risico-kans-x-effect-gratis/