

Experiment veilig toetsen in de cloud bij HBO-V: eindrapport

Michiel van Geloven, 12 maart 2014

Na een voorbereiding van enkele maanden werd in november 2013 een praktijktest uitgevoerd om na te gaan of het mogelijk is om de toetsomgeving van Leerstation Zorg afdoende te beveiligen voor summatieve toetsing. Het experiment is uitgevoerd door Leerstation Zorg (coördinatie), Infoland (ontwikkeling add-on summatief toetsen), de vijf deelnemende hogescholen: Hogeschool Rotterdam, Hogeschool Utrecht, Hogeschool Arnhem Nijmegen, NHL Hogeschool en Saxion, ondersteund door SURF (advies en verslaglegging).

Dit experiment is uitgevoerd in het kader van het *Plan van aanpak gemeenschappelijke infrastructuur digitaal toetsen hoger onderwijs*, dat een onderdeel is van het Programma Toetsing en Toetsgestuurd Leren van SURF. Het experiment was een uitbreiding op het project *Body of Knowledge and Skills, verbreden en verbinden* (werktitel: Toetsen met de BoKS), een groot project onder leiding van Hogeschool Rotterdam en eveneens onderdeel van het Programma Toetsing en Toetsgestuurd Leren van SURF.

In dit eindrapport behandelen we achtereenvolgens de *lessons learned* op vier aspecten:

1. techniek
2. veiligheid
3. organisatie en beheer
4. business case (kosten en baten)

Techniek

Het experiment was mede aanleiding om een specifieke add-on ‘summatief toetsen’ te ontwikkelen bij het toetssysteem van Leerstation Zorg. Deze add-on kan door de hogescholen gebruikt worden zonder dat zij daarvoor aanpassingen in hun eigen infrastructuur hoeven doen. De add-on is ontwikkeld door de ICT-partner van Leerstation Zorg: Infoland.

Voor summatief toetsen is het doorgaans wenselijk of vereist, dat studenten uitsluitend toegang hebben tot de toetsapplicatie en niet tot andere software zoals een webbrowser of e-mail. Hiervoor wordt een zgn. lock-down browser ingezet. In het kader van dit experiment is hiervoor de software van SiteKiosk gebruikt. Deze moet correct geconfigureerd worden en blijkt dan een afdoende beveiliging te bieden (zie onder ‘veiligheid’).

Voor de beheerder/hoofdsurveillant is een aparte ‘console’ in de toetssoftware beschikbaar, waarmee hij/zij de studenten na controle (ID-kaart bijv.) toegang kan geven tot de toets. Op twee locaties werd hiervoor gewerkt met een barcode-scanner. Dit werkte vlot en handig en de wens is uitgesproken om dit meer te gaan doen.

Tijdens het experiment werkten ongeveer 120 studenten op vijf verschillende locaties tegelijk met de toetssoftware. Er zijn geen afwijkingen in de performance van de software geconstateerd. Wel is er een fout in de software aangetroffen waardoor studenten op sommige momenten korte tijd geen antwoord konden invoeren. Dit probleem is inmiddels verholpen.

Tijdens het experiment was de systeemontwikkelaar van de leverancier (Infoland) standby en voor de onderlinge communicatie was een Whatsapp-groep ingericht. Hierdoor werden enkele kleine problemen direct verholpen.

Om de add-on summatief toetsen verder uit te rollen zal het nodig zijn om de beheermodule door te ontwikkelen, onder meer verbetering van de gebruikersinterface. Daarnaast is te overwegen uit veiligheidsoverwegingen een vorm van dubbele authenticatie in te bouwen (bijv. met SMS of een token).

In het kader van het experiment is de toetsomgeving gekoppeld met SURFconext. Het vroeg een aanmerkelijke inspanning om dit volledig te implementeren (vooral aan de zijde van Infoland), maar tijdens de uitvoering van de toets is gebleken dat de beoogde functionaliteit doet wat hij moet doen. Om optimaal van SURFconext gebruik te kunnen maken zou ook functionaliteit beschikbaar moeten zijn om (toets)groepen langs deze weg te onderscheiden.

Veiligheid

Het kernaspect van het experiment was te onderzoeken, of er met de toetssoftware van Leerstation Zorg op een veilige manier een summatieve toets afgenomen kan worden. Hiervoor zijn in essentie langs twee lijnen voorbereidingen getroffen: de ontwikkeling van de add-on summatief toetsen binnen de toetssoftware en de installatie van een lock-down browser op de toetswerkplekken.

Bij de beveiliging van toetsen is sprake van een 'keten', waarin verschillende partijen een verantwoordelijkheid hebben:

1. de softwareleverancier / de hostende partij: deze moet zorgen dat de hardwareomgeving en de software goed is beveiligd
2. de IT-afdeling van de instelling: deze is verantwoordelijk voor een adequate inrichting van de toetswerkplekken met o.a. een lock-downbrowser
3. de afdeling gebouwbeheer van de instelling: deze is verantwoordelijk voor de inrichting (meubilair) van de toetszalen, denk aan 'schotten' tussen de pc's, goede verlichting, klimaatbeheersing, stroomvoorziening etc.
4. de toezichthouder: deze moet zorgen – in samenwerking met de surveillanten – voor een ordentelijk verloop van de toets, denk aan controle van de ID-kaart van de studenten, spieken, etc.

Om de veiligheid te testen is een externe partij gevraagd een zgn. ethical hack uit te voeren. Hierbij wordt door experts geprobeerd om – onder andere met behulp van specifieke tools – geprobeerd om bijv. ongeoorloofd mutaties aan te brengen in toetsresultaten, toetsvragen te 'stelen', in te loggen onder een andere naam, of om de software drastisch te vertragen.

Experts van de firma Insite Security hebben twee verschillende tests uitgevoerd:

1. Is een student in staat de toets te manipuleren? Kan de student bijvoorbeeld via Google naar antwoorden zoeken of toetsvragen kopiëren naar een usb-stick? Dit is op drie van de deelnemende hogescholen geprobeerd.
2. Kan iemand voor, tijdens of na de toets onrechtmatig toegang krijgen tot het online toetssysteem om bijvoorbeeld de vragen te bemachtigen of om de resultaten te manipuleren?

Het online toetssysteem LMS van Leerstation Zorg was binnen de beschikbare randvoorwaarden (beperkte hoeveelheid tijd en geld) niet te hacken. Op twee van de drie instellingen lukte het de hackers niet om de toets-pc's te manipuleren dankzij de goed geconfigureerde lock-down browser. Bij één instelling was de lock-down browser niet goed geconfigureerd. Hierdoor hadden de hackers vrij toegang tot de pc, alle programma's en websites waaronder Google. Daarnaast waren usb-poorten en de cd-rom te gebruiken.

De instellingen en de leverancier van het toetssysteem hebben suggesties gekregen voor een nog betere beveiliging. Zo merkten de hackers op dat de toets-pc's niet in een apart (IP-)netwerk waren ingedeeld. De toetsomgeving kan dan via elke pc in het gebouw benaderd worden. In theorie is het dan mogelijk dat een andere student dan degene in het toetslokaal de toets maakt. Instellingen kunnen de beveiliging met aparte netwerksegmenten dus nog verder verbeteren.

Deze uitkomst laat zien dat de cloud-leverancier niet als enige verantwoordelijk kan zijn voor de beveiliging in de gehele toetsketen: de verantwoordelijkheid voor een correcte inrichting van de toetswerkplekken ligt bij de instelling. Ook laat het experiment zien dat de toepassing van een goede lock-down browser een afdoende beveiliging biedt op de toetswerkplek: studenten kunnen niet ongeoorloofd andere software gebruiken en ze hebben geen toegang tot usb-sticks e.d.

In het experiment zijn fysieke beveiligingsmaatregelen, zoals schotten tegen afkijken, buiten beschouwing gelaten. Dat geldt ook voor verschillende andere, algemene aspecten die bij summatieve toetsen doorgaans wenselijk of vereist zijn, zoals de identificatie van de deelnemende studenten.

Organisatie en beheer

In beginsel vraagt een summatieve toets van Leerstation Zorg geen andere maatregelen dan een 'normale' summatieve toets, zoals de instelling gewend is die te houden. Wel is het aan te raden de surveillant(en) specifiek te instrueren, omdat de procedure van aan- en afmelden van studenten waarschijnlijk afwijkt van wat ze gewend zijn bij andere toetssystemen.

Tijdens de voorbereidingen en uitvoering van het experiment is een aantal punten opgevallen:

- Het kostte bij sommige instellingen veel moeite om contact te krijgen met de functionaris die verantwoordelijk is voor informatiebeveiliging. Het lijkt erop dat de (rol van) *security officer* niet altijd even bekend is bij de hogescholen.

- We hebben enige koudwatervrees gezien rondom de ethical hack: enkele instellingen waren ongerust dat hun infrastructuur door deze activiteit zou worden beschadigd. Hoewel de hackers zorgvuldig te werk gaan, bestaat er een kleine kans dat dit inderdaad gebeurt. In het experiment zijn geen problemen ontstaan door de activiteiten van de hackers.
- Er was veel afstemming nodig met de IT-afdelingen van de respectievelijke instellingen om de inrichting van de toetswerkplekken met een adequate lock-down browser op orde te krijgen. Dit komt waarschijnlijk mede doordat sommige instellingen als beleid hebben dat alleen de gezamenlijk gekozen toetssoftware wordt ondersteund.
- De itembank van Leerstation Zorg wordt momenteel hoofdzakelijk ingezet voor formatieve toetsing. In de loop van het project Toetsen met de BoKS is de vraag aangewakkerd naar meer summatieve toetsing – wat in veel gevallen niet eenvoudig te organiseren is, vooral door een gebrek aan grotere pc-zalen waar veilig getoetst kan worden. Buiten de scope van het experiment wordt nagedacht over oplossingsrichtingen met laptops, iPads of print&scan.
- De vraag naar summatief toetsen stelt andere, meer complexe eisen aan de inrichting van de itembank (delen moeten afgeschermd worden bijv.) en leidt ook tot nieuwe afstemmingsvraagstukken (o.a. met examencommissies).

Business case

Tot dusver is de itembank van Leerstation Zorg overwegend ingezet voor formatieve toetsing. Er zijn – onder meer in het kader van het experiment – verschillende opties in beeld om summatieve toetsing op substantiële schaal mogelijk te maken. Hieronder bespreken we eerst een aantal aspecten van summatief toetsen die specifiek zijn voor Leerstation Zorg. Aan het eind van dit hoofdstuk gaan we kort in op een aantal varianten om vanuit de itembank van Leerstation Zorg de praktische organisatie van summatief toetsen in te vullen.

Summatief digitaal toetsen & Leerstation Zorg

Zonder in detail te treden¹ geven we hier enkele aandachtspunten die van invloed kunnen zijn op de business case van summatief digitaal toetsen met Leerstation Zorg. Die business case zal per hogeschool verschillen.

Aan de opbrengstenkant zien we bij summatief toetsen met de toetsbank van Leerstation Zorg de volgende essentiële aspecten: de gegarandeerde (hoge) kwaliteit van de toetsvragen en het feit dat de toets niet ‘ergens in een bureaulade’ ligt, maar in een gezamenlijk systeem wordt geborgd. Bovendien is er geen correctiewerk en dus -tijd, omdat de toetsen door de software worden nagekeken. Daardoor kan de uitslag doorgaans snel bekend worden gemaakt (dat geldt zowel bij digitale afname als bij de print&scan-optie). De kwalitatieve aspecten laten zich lastig in geld uitdrukken, voor de winst op nakijktijd kan elke hogeschool voor zichzelf bepalen wat hier de opbrengst kan zijn.

¹ daarvoor verwijzen we graag naar de “Quickscan kosten & baten van digitaal toetsen”, uitgave SURF. Zie <http://tinyurl.com/m7lpy2e>. In de loop van 2014 verschijnt bij SURF ook de “Business case van digitaal toetsen”.

Daar staat tegenover dat een instelling hogere kosten maakt, in ieder geval vanwege de licentie op de add-on summatief toetsen. Verder moet in er rekening mee worden gehouden dat in hogescholen soms een gemeenschappelijk toetsstelsel in gebruik is – in beginsel ook voor de zorgopleidingen, die daarmee in feite dubbele (licentie)kosten hebben. Ook het interne beheer van verschillende systemen kan leiden tot extra kosten.

Bij digitale afname is het zaak goede afspraken te maken met de IT-afdeling van de hogeschool: de pc's in de toetszaal moeten juist geconfigureerd zijn (dat gaat in het bijzonder over de lock-downbrowser). Deze configuratie is in de praktijk vaak (licht) afwijkend van de vereiste configuratie voor andere toetssoftware en dat is een belangrijk punt om rekening mee te houden. Verder is het een belangrijke vraag, hoeveel studenten tegelijk een digitale toets kunnen doen. Als dat aantal kleiner is dan de totale populatie, dan is dit in elk geval een logistieke uitdaging (zalenplanning). Daarnaast zijn er dan meer toetsen nodig, omdat het nauwelijks mogelijk is om verschillende groepen dezelfde toets voor te zetten (zie ook verderop).

Als de aantallen groot zijn en de digitale toetslokalen klein, dan is print&scan wellicht de beste optie. Overwogen kan worden om uit te wijken naar een collega-instelling die beschikt over een grote toetszaal (dat zijn er nu nog vrij weinig, maar naar verwachting zal het aantal groeien; de universiteiten lijken hierin voorop te lopen).

Een belangrijk punt van aandacht is de hoeveelheid benodigde items: als er wordt geput uit een gezamenlijke, landelijke itembank voor summatieve toetsen én elke instelling kiest zijn eigen toetsmoment, dan zijn er heel veel vragen nodig. Doorgaans wordt als regel gehanteerd dat een vraag maximaal eens per drie jaar summatief kan worden gebruikt. Als elke hogeschool jaarlijks twee toetsen afneemt met 100 vragen, dan zijn al er $2 \times 100 \times 17 = 3400$ vragen *per jaar* nodig. Een alternatieve oplossing is dat er afspraken worden gemaakt over afname op een beperkt aantal momenten: verschillende hogescholen toetsen tegelijk.

Voor gebruikersbeheer kan in beginsel gebruik gemaakt worden van de functionaliteit die SURFconext biedt. Om dit naar de toekomst te garanderen is het een vereiste dat Leerstation Zorg een samenwerkingsovereenkomst aangaat met SURFmarket. Dit zal betekenen dat de instellingen voortaan hun licenties afnemen via SURFmarket. Als deze stap wordt gezet, dan betekent dit:

- a. Instellingen die zijn aangesloten op SURFconext kunnen hun gebruikersbeheer voor Leerstation Zorg via deze voorziening laten lopen en hoeven hiervoor geen aparte oplossing meer te gebruiken
- b. De licenties van Leerstation Zorg zullen dan via SURFmarket moeten lopen en ook aldaar worden besteld. SURFmarket rekent een kleine opslag om de kosten te dekken (inclusief SURFconext, dat is inbegrepen in het tarief). De opslag is in 2014: 4,5%.

Toetsafname: zes varianten

Tot slot geven we een korte analyse van voor- en nadelen van verschillende opties voor de afname van digitale toetsen.

Optie 1: 'standaard pc-zalen'

Vrijwel elke hogeschool beschikt over een aantal pc-lokalen die gebruikt worden voor onderwijs en andere doeleinden. Deze zalen zijn in beginsel ook te gebruiken voor digitaal toetsen.

Voordelen van deze oplossing:

- Er is geen aparte investering nodig, de zalen worden optimaal benut.
- Deze zalen zijn doorgaans gesitueerd in de directe nabijheid van de opleidingen die er gebruik van maken.

Daaraan kleven echter enkele nadelen:

- Deze zalen zijn vaak beperkt van omvang: er kunnen hooguit enkele tientallen studenten tegelijk een toets doen.
- Deze zalen zijn doorgaans niet ingericht op digitaal toetsen: er zijn geen voorzieningen om spieken tegen te gaan; dit is meestal op te lossen met mobiele schotten, maar dat is wel 'gedoe'.
- PC's voor digitaal toetsen vereisen soms een specifieke configuratie, die mogelijk strijdig is met de eisen die het andere, 'gewone' gebruik stelt.
- Het is soms lastig om deze zalen vrij te roosteren voor een digitale toets.
- Deze zalen moeten idealiter enkele uren voorafgaand aan de toets worden vrijgeroosterd om de werkplekken te controleren en zo nodig te installeren.

Optie 2: 'specifieke toetszalen'

In dit model wordt speciaal voor digitaal toetsen een computerlokaal ingericht, dat niet voor andere doelen gebruikt wordt. Bij een toenemend aantal instellingen gaat het hier om een zaal van flinke omvang met enkele honderden werkplekken.

Voordelen van deze oplossing:

- Een dedicated toetszaal kan optimaal voor toetsing worden ingericht, zowel de IT-inrichting als het meubilair.
- Er is geen 'beschikbaarheidsconcurrentie' met het onderwijs.
- De fysieke bewaking van de zaal en de pc's kan optimaal worden ingeregeld.

Daaraan kleven echter enkele nadelen:

- Een dergelijke zaal is relatief duur om in te richten.
- De kans bestaat dat zo'n zaal slechts gedurende enkele weken per jaar gebruikt wordt (al laat de praktijk zien dat toetszalen ook buiten de vaste toetsweken volop gebruikt worden, o.a. voor formatieve toetsing).

- Als een instelling één zo'n toetszaal inricht, dan bevindt deze zich mogelijk op een andere locatie van de opleiding.
- De meeste instellingen concentreren alle toetsen in een beperkt aantal toetsweken; dit leidt al snel tot piekbelasting van de toetszalen en mogelijk tot capaciteitsproblemen.

Optie 3: 'mobiele laptop-karren'

In het kader van het project Toetsen met de BoKS is bij enkele hogescholen bij wijze van pilot gewerkt met 'toetskarren', speciaal ingerichte karren met laptops die alleen gebruikt worden voor summatief toetsen voor Leerstation Zorg. Dit is goed bevallen, en sommige instellingen hebben inmiddels de toetskar-capaciteit uitgebreid. Dankzij de add-on summatief toetsen kan deze oplossing nu werken via de cloud, wat een belangrijk risico beperkt: voorheen moest de toets met een losse usb-stick worden geïnstalleerd.

Voordelen van deze oplossing:

- De pc's worden optimaal voor toetsing ingericht en blijven dat ook, omdat ze niet voor andere doelen gebruikt worden.
- Er is geen 'beschikbaarheidsconcurrentie' met regulier gebruik van de pc's.
- De fysieke bewaking van de zaal en de pc's kan optimaal worden ingeregeld.
- De karren zijn flexibel in te zetten op vele locaties.
- Laptops zijn per definitie minder afhankelijk van netstroom.

Daaraan kleven echter enkele nadelen:

- De karren zijn niet heel kostbaar, maar het beheer ervan en de 'uitrol' en het 'inpakken' vraagt telkens een flinke inspanning.
- De kans bestaat dat zo'n toetskar slechts gedurende enkele weken per jaar gebruikt wordt.
- De beveiliging van het geheel vraagt specifieke aandacht.
- Voor hele grote groepen minder geschikt.

Optie 4: 'tablets van de hogeschool'

In plaats van laptops is het wellicht een optie om tablets in te zetten. Als deze in eigendom zijn van de hogeschool en ze worden zorgvuldig beheerd, dan is het wellicht mogelijk om 'in control' te blijven van deze apparatuur.

Grosso modo geldt voor deze oplossing dezelfde voor- en nadelen als bij de toetskarren (optie 3). Daar komt bij dat er op dit moment (2014) nog geen sluitende oplossing is om tablets goed genoeg te beveiligen (er is bijv. geen adequate lock-down browser beschikbaar voor dergelijke apparatuur).

Optie 5: 'BYOD'

Het lijkt aantrekkelijk om studenten met hun eigen apparatuur toetsen te laten maken. De instelling hoeft dan geen pc's in te richten, aan te schaffen of vrij te houden voor toetsing. Vooralsnog is het gebruik van 'allerlei' apparatuur eigenlijk niet bruikbaar voor (summatief) toetsen.

Drie redenen om BYOD niet in te zetten voor summatief toetsen:

1. omdat elke student weer een ander apparaat met andere software kan hebben, kunnen (en waarschijnlijk: zullen) er bij sommige problemen optreden met het correct functioneren van de toetssoftware.
2. er is op dit moment geen goede oplossing om de apparatuur adequaat te beveiligen. Potentiële oplossingen met bijv. usb-sticks bleken bij eerdere experimenten niet te voldoen. Wellicht komt hiervoor binnen enkele jaren een oplossing.
3. opleidingen of instellingen stellen steeds vaker eisen aan het beeldscherm van een toets-werkplek, bijv. minimale schermgrootte. Tablets en laptops voldoen hier vaak niet aan.

Optie 6: 'print & scan'

Het lijkt een stap terug in de tijd: in plaats van meerkeuzevragen op het beeldscherm wordt teruggevallen op een oud, maar beproefd mechanisme: toetsen afdrukken en studenten hun antwoorden op voorgedrukte formulieren laten invullen. Deze formulieren worden gescand en dan alsnog automatisch nagekeken. Dit vraagt een andere voorbereiding (bijv. het kopiëren van de vragenstukken en antwoordformulieren) en het natraject is arbeidsintensiever: de stapel ingeleverde formulieren moet worden gescand en dat vraagt enig handwerk, net als de nacontrole.

Voordelen van deze oplossing:

- geen pc's nodig: kan in elk (toets)lokaal
- niet gevoelig voor allerlei techniek-storing
- vereist minder investering
- alle digitale mogelijkheden van een gezamenlijk "summatieve" itembank onderhouden worden gebruikt

Daaraan kleven echter enkele nadelen:

- voordelen van online toetsen vervallen weer, denk aan hoogwaardige beelden, video, bijzondere interacties, maar ook de mogelijkheid om vragen en antwoordalternatieven te 'husselen'
- de logistiek van print&scan moet zorgvuldig worden voorbereid en het scannen vraagt kennis van zaken; de instelling moet over de juiste apparatuur en software beschikken
- het past minder goed in het imago van 'modern onderwijs' verzamelen van analyses voor de gezamenlijkheid vraagt om een extra slag