Audit: Beveiliging Digitale Examens

Hans Doffegnies
Directeur dienst Facilities
Summa College

Ernst Jan Zwijnenberg
Unitmanager ICT-Security
Hoffmann Bedrijfsrecherche

Hoffmann Bedrijfsrecherche bv

http://www.youtube.com/watch?v=Wq-wN7LYKXU

Regio met grote ambities

Onze regio, Brainport regio Eindhoven,
is een van de meest dynamische en succesvolle regio's van Nederland en heeft grote ambities. De vakmensen die wij opleiden zijn onmisbaar om die ambities te verwezenlijken.

Ruim **40%** van de werkenden in onze regio heeft een mbo-diploma. Wij zijn met afstand de belangrijkste leverancier van deze vakmensen.

Afbeelding Brainport.nl

SUMMA College

Wij zijn een toonaangevende organisatie voor middelbaar beroepsonderwijs in **Brainport regio Eindhoven** waar jongeren en volwassenen zich thuis voelen.

In **hechte samenwerking** met bedrijven en instellingen leveren wij uitdagend en kwalitatief hoogwaardig onderwijs.

Wij staan voor een succesvolle studie en carrière van onze studenten, gebaseerd op vakmanschap en persoonlijke groei, voor nu en in de toekomst. Daarmee bouwen wij aan de **welvaart in de regio**.

Hoffmann helpt u om uw organisatie te beschermen tegen fraude van binnenuit of van buitenaf.

Denk aan onterecht ziekteverzuim, interne diefstal en oneigenlijk internetgebruik. Onze filosofie daarbij is dat uw medewerkers zowel de zwakste als de sterkste schakel in uw beveiliging tegen fraude zijn

SUMMA College

Facts & figures

- Aantal studenten: ± 16.000
- Aantal medewerkers: ± 1.500
- Aantal opleidingen: ± 250
- Aantal diploma's per jaar: ± 6.000
- Aantal locaties: 14 in Eindhoven, 1 in Veldhoven
- 2013: 61% van niveau 4 stroomt door naar hbo

Hoffmann heeft drie afdelingen: Bedrijfsrecherche, ICT-Security en Consultancy & Opleidingen.

Deze afdelingen vullen elkaar in de verschillende diensten perfect aan. En omdat wij een brede expertise in huis hebben, kunnen wij al uw beveiligings- en fraudevragen geheel zelfstandig beantwoorden.

Agenda:
Audit Beveiliging Digitale Examens

1. Aanleiding van de Audit
2. Waarom Keuze Hoffmann Bedrijfsrecherche
3. Opzet van de Audit
4. Uitvoering van de Audit
5. Bevindingen van de Audit
6. Aanbevelingen n.a.v. de Audit
7. Hoe nu verder

Aanleiding van de Audit

Examenfraude: is digitaal veiliger dan papier?

Nieuw protocol voor examentijd

‘Examenfraude ROC Amsterdam - 825 examens ongeldig’

Veiligheidsprotocol en examenfraude

Geleerde lessen na examenfraude

Mogelijke examenfraude op Haagse Hogeschool

Zeven studenten van de Haagse Hogeschool hebben mogelijk gefraudeerd met tentamens. Zij zijn daarom de komende twee weken geschorst.

Beantwoording Kamervragen examenfraude ROC Amsterdam

Antwoorden van minister Bussemaker (OCW) op vragen van het Kamerlid Jadnanansing (PvdA) over het bericht 'Grote examenfraude ROC Amsterdam'.

Waarom heeft het Summa College Hoffmann Bedrijfsrecherche in de arm genomen?

- College van Bestuur van het Summa College zag sense of urgency met betrekking tot berichtgeving in de pers
- College van Bestuur van het Summa College wilde weten hoe de vlag er bij hing bij de afname van (digitale examens)
- Hoffmann bedrijfsrecherche heeft brede expertise
- Hoffmann bedrijfsrecherche was/is betrokken bij fraudegevallen bij (digitale) examens in het onderwijs
- Hoffmann bedrijfsrecherche geeft adviezen om fraude binnen je organisatie te voorkomen.

Opzet Onderzoek I

Scope:

- Het onderzoek dient gericht te zijn op het proces van ontvangen, verspreiden en afnemen van de Centraal Ontwikkelde Examens (COE) van het Cito.

- Het onderzoek van Hoffmann heeft zich gericht op zowel de technische aspecten (digitaal) als de organisatorische maatregelen zoals deze genomen zijn binnen het Summa College inzake afname van digitale (COE) examens.

Opzet Onderzoek II

Het onderzoek is in **vier stappen** uitgevoerd, namelijk:

- Interviews met functionarissen die een rol spelen in het examenproces (COE);
- Bestuderen documenten en borging procesgang;
- Uitvoeren audit om de effectiviteit van bepaalde beveiligingsmaatregelen op operationeel niveau te onderzoeken;
- Testen van de ICT-beveiliging van het Summa College (pentesten).

Bevindingen I

Documentatie en borging procesgang

Het procesdocument dat het Summa College hanteert omschrijft zeer duidelijk de gang van zaken betreffende het COE-examen.

De procesgang wordt verder gevolgd en vastgelegd met het ‘Logboek COE Nederlands en rekenen’ en na afloop van een examen wordt middels het ‘Procesverbaal Afname centraal examinering Nederlands en rekenen’ vastgelegd wie het examen heeft afgenomen en of er eventuele bijzonderheden zijn.

Bevindingen II

Toewijzen verantwoordelijkheden proceseigenaren

Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd. Een en ander staat duidelijk omschreven in het procesdocument, zoals hierboven is aangegeven. De geïnterviewden waren allen goed op de hoogte van de taken en verantwoordelijkheden.

Beveiligingsbewustzijn

Alle geïnterviewden die betrokken zijn bij het organiseren of afnemen van de COE, inclusief externe inhuurkrachten (surveillanten), zijn goed op de hoogte van de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en het voorkomen van examenfraude. Er zijn in het verleden centrale briefings gehouden voor surveillanten, waarbij deze voorafgaande aan de COE, op de hoogte werden gebracht over de gang van zaken en de procedures.

Bevindingen III

Fysieke beveiliging en beveiliging van apparatuur

IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden.

Vanuit de interviews is bekend geworden dat de examenlokalen puur bestemd zijn voor het afnemen van het COE.

Procedure toegangsbeveiliging examens

Er zijn procedures om senior examenmedewerkers toegang te geven tot de Cito-examens (packages) die ze voor het roosteren nodig hebben. Hiervoor krijgen zij een persoonlijke brief met persoonlijke inlogcode, waarmee zij de examendocumenten op de server van het Summa College kunnen downloaden. Deze serverruimte is beperkt toegankelijk. Zelfs nadat deze examens zijn gedownload op de server van het Summa College, is het niet mogelijk (zeer moeilijk) inzage te krijgen in de examens. Deze zijn namelijk door middel van versleuteling beveiligd.

Bijlage: Fraude scenario risico matrix

Risico-identificatie			Risico analyse	Risico beperkend advies
Incident-scenario	**Fraude-risico**	**Genomen maatregelen**	**Score (kans)**	**Advies**
Fraude door senior examenmedewerker COE	1. Examens vooraf kopiëren en distribueren 2. Datum voor leerling aanpassen en apart laten maken (dummy planning)	Algemene maatregelen - Medewerkers Summa die betrokken zijn bij de uitvoering van de examinering hebben zich geconformeerd aan een geheimhoudingsverklaring - Activiteiten rondom examens vinden plaats met vierogenprincipe, zodat onregelmatigheden onderkend zullen worden Specifieke maatregelen 1. Examens worden encrypted binnengehaald op server vanaf CITO; senior examenmedewerker kan zelf de examens niet openen (zie ook digitaal onderzoek); 2. Indien leerling het examen op een ander tijdstip maakt, dan zal dit opvallen doordat dit als uitzondering wordt vastgelegd in het systeem.	Laag	- Breng extra controle in gericht op planning/roostering door senior examenmedewerker, zodat eventuele dummy-planning zo goed als onmogelijk wordt

		Aandachtspunten - Het lijkt erop dat de planning van de examens voornamelijk door de senior examenmedewerker gebeurt. Het is niet duidelijk gebleken dat hier een extra controle op plaatsvindt.		
Fraude door IT-deskundige / systeembeheerder COE	1. IT-medewerker verkrijgt toegang tot examenbestanden en kopieert deze voor distributie 2. IT-medewerker past planning aan voor individuele kandidaat	Algemene maatregelen - Medewerkers Summa die betrokken zijn bij de uitvoering van de examinering hebben zich geconformeerd aan een geheimhoudingsverklaring Specifieke maatregelen 1. Examens worden encrypted binnengehaald op server vanaf CITO; IT-medewerker kan zelf de examens niet openen (zie ook digitaal onderzoek); 2. Indien leerling het examen op een ander tijdstip maakt, dan zal dit opvallen doordat dit als uitzondering wordt vastgelegd in het systeem. Aandachtspunten - Het is onduidelijk hoe de IT-medewerkers worden gecontroleerd en of er forensische sporen achterblijven bij misbruik door deze medewerkers	Laag	- Breng extra controle in gericht op planning/roostering door senior examenmedewerker, zodat eventuele wijziging in planning zo goed als zeker opgemerkt wordt - Check 'forensic readiness' zodat misbruik door IT-medewerkers terug te traceren valt

Fraude door Surveillant	1. Surveillant helpt kandidaat, bijvoorbeeld door antwoorden geven, of 'knijpt oog dicht' bij gebruik spiekbrief 2. Surveillant werkt mee bij binnenlaten vervangende student (identiteitsfraude)	Algemene maatregelen - Surveillanten die betrokken zijn bij de uitvoering van de examinering hebben zich geconformeerd aan een geheimhoudingsverklaring die wordt uitgegeven door het uitzendbureau (Randstad) Specifieke maatregelen - Er wordt gewerkt met twee surveillanten (vierogenprincipe) - Bij aanmelding is identificatie van leerling verplicht Aandachtspunten - Surveillanten worden gescreend door Randstad. Het is onduidelijk of deze screening zorgvuldig wordt uitgevoerd - Randstad stemt geheimhoudingverklaringen af met aangenomen kandidaten, echter overlegt dit niet met het Summa College. - ID-bewijs van Summa College is gemakkelijk na te maken, of extra pas kan gemakkelijk aangevraagd worden. Fraude met dit ID-bewijs is gemakkelijk - ID-controle door surveillanten geschiedt voornamelijk op naam en studentennummer. Foto wordt niet (voldoende) gecontroleerd	**1.Laag** **2.Medium**	- Identificatie via schoolpas is niet sluitend! Deze passen zijn relatief eenvoudig na te maken, of zelfs dubbel te laten vervaardigen op school (extra pas maken). De enige goede identificatie is mogelijk via officieel document (rijbewijs, paspoort of ID bewijs). Surveillanten dienen daarbij gericht te controleren op de foto op dit document. - Summa blijft verantwoordelijk voor controle op getekende geheimhoudingsverklaring. Breng extra controle in om zeker te stellen dat surveillanten deze ook daadwerkelijk hebben ondertekend (kopie).

Fraude door leerling	1. Kandidaat stuurt een bevriende student om examen te maken 2. Kandidaat spiekt tijdens examen	Algemene maatregelen - Surveillanten kunnen scherp toezicht houden - Examenlokaal kent goede faciliteiten, die (structureel) spieken zeer moeilijk maken - Examens kunnen verschillen per leerling Specifieke maatregelen - Er wordt gewerkt met twee surveillanten - Bij aanmelding is identificatie van leerling verplicht. - Vorm waarin examens worden afgenomen zorgen ervoor dat spieken niet veel oplevert Aandachtspunten - ID-bewijs van Summa College is gemakkelijk na te maken, of extra pas kan gemakkelijk aangevraagd worden. Fraude met dit ID-bewijs is gemakkelijk - ID-Controle door surveillanten geschiedt voornamelijk op naam en studentennummer. Foto wordt niet (voldoende) gecontroleerd	**Medium**	- Identificatie via schoolpas is niet sluitend! Deze passen zijn relatief eenvoudig na te maken, of zelfs dubbel te laten vervaardigen op school (extra pas maken). De enige goede identificatie is mogelijk via officieel document (rijbewijs, paspoort of ID-bewijs). Surveillanten dienen daarbij gericht te controleren op de foto op dit document.

Doel en Scope van Technisch Digitaal Onderzoek

Doel van de penetratietest was het testen van de IT-infrastructuur van het Summa College op kwetsbaarheden waardoor hackers of kwaadwillenden onrechtmatig over bedrijfsgevoelige gegevens, in het bijzonder de Centraal Ontwikkelde Examens, zouden kunnen beschikken.

De scope van het onderzoek is een beveiligingsonderzoek op de IT-infrastructuur van het Summa College aan de hand van de blackbox-methode en greybox-methode. Hierbij worden alle zichtbare systemen van het Summa College gecontroleerd.

Hoewel de uiteindelijke doelstelling van het onderzoek is te bepalen in welke mate de Centraal Ontwikkelde Examens voldoende beveiligd zijn tegen fraude, is het van groot belang de omringende infrastructuur op onvolkomenheden te onderzoeken. Immers, de mogelijkheid kan bestaan dat juist via deze systemen een kwaadwillende zichzelf toegang kan verschaffen tot deze examens.

Bevindingen technisch digitaal onderzoek

Deze bevindingen zijn strikt vertrouwelijk en kunnen helaas niet worden gedeeld.

Na jaren praktijkervaring adviseert Hoffmann (en tevens alle security standaarden) om periodiek de IT infrastructuur te laten testen op kwetsbaarheden.

METEN=WETEN

Hoe staat uw organisatie ervoor op het gebied van ICT Security?

Bezoek ons ook op:

www.summacollege.nl

www.hoffmannbv.nl
www.fraude.nl

www.facebook.com/SummaCollege

www.twitter.com/summacollege

www.youtube.com/user/SummaCollegeFilm

www.plus.google.com/+SummaCollegeEindhoven