COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Stichting Hogeschool van Arnhem en Nijmegen

Onderzoek naar de beveiliging van persoonsgegevens van studenten

z2011-01006

Rapport definitieve bevindingen

januari 2013

DATUM 17 januari 2013

INHOUDSOPGAVE

1. SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzocht in hoeverre de Stichting Hogeschool van Arnhem en Nijmegen (hierna: de HAN) passende technische en organisatorische maatregelen heeft getroffen om persoonsgegevens van studenten te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking als bedoeld in artikel 13 van de Wet bescherming persoonsgegevens (Wbp). Meer specifiek is het onderzoek toegespitst op het informatiesysteem X. In het informatiesysteem X worden - onder meer - rasgegevens van studenten verwerkt. Dit zijn bijzondere persoonsgegevens in de zin van artikel 16 Wbp.

Bij de toetsing van de getroffen beveiligingsmaatregelen door de HAN aan artikel 13 Wbp is de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007) als meetinstrument gebruikt.

Tijdens het onderzoek heeft het CBP aanvankelijk geconstateerd dat de HAN onvoldoende maatregelen had getroffen ten aanzien van de beveiligingsaspecten 'Beheer van toegangsrechten van gebruikers', 'Beoordeling toegangsrechten', 'Logging en controle' en 'Audit informatiebeveiliging'. De HAN handelde hierdoor in strijd met artikel 13 Wbp. Naar aanleiding van het rapport van voorlopige bevindingen heeft de HAN alsnog de vereiste beveiligingsmaatregelen getroffen, met uitzondering van het beveiligingsaspect 'Logging en controle'.

Ten aanzien van de onderzochte beveiligingsaspecten 'Informatiebeveiligingsbeleid', 'Toegangsbeheersing', 'Blokkeren en aanpassen van toegangsrechten', 'Gebruik van wachtwoorden', 'SQL-injectie en Cross-Site Scripting (XSS)', 'Cryptografische beheersmaatregelen' en 'Beheer van informatiebeveiligingsincidenten' heeft het CBP geen overtredingen geconstateerd.

2. INLEIDING

2.1 Aanleiding onderzoek

In het hoger onderwijs wordt een groot aantal persoonsgegevens - zoals naw-gegevens, bijzondere persoonsgegevens in de zin van artikel 16 Wbp en gegevens betreffende de studievoortgang - van studenten verwerkt. Het gaat hierbij om een grote groep betrokkenen. Zo waren bij de HAN in 2011 30.365 studenten ingeschreven.[1] De verwerking van persoonsgegevens van studenten vindt veelal op geautomatiseerde wijze plaats, hetgeen strenge eisen stelt aan de informatiebeveiliging.

In de media zijn de afgelopen jaren veel berichten verschenen over het lekken van studentgegevens door hoger onderwijsinstellingen. Daarnaast ontvangt het CBP steeds vaker signalen over datalekken, bijvoorbeeld ingevolge van SQL-injectie[2] of XSS[3]. Betrokken studenten kunnen hierdoor ernstige gevolgen ondervinden, met name indien het gaat om bijzondere persoonsgegevens of andere gevoelige gegevens. Het is derhalve van groot belang dat hoger onderwijsinstellingen passende maatregelen ten uitvoer leggen om persoonsgegevens van studenten te beveiligen.

Bovenstaande is voor het CBP aanleiding geweest om een onderzoek te starten naar de informatiebeveiliging bij hoger onderwijsinstellingen.

2.2 Doel en reikwijdte onderzoek

De HAN verwerkt persoonsgegevens van studenten op zijn interne informatiesystemen. Het onderzoek beoogt vast te stellen of de HAN passende technische en organisatorische maatregelen heeft getroffen om deze persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De beveiliging dient zich uit te strekken tot alle onderdelen van het proces van gegevensverwerking, vandaar dat het CBP een breed scala van informatiebeveiligingsaspecten heeft onderzocht.

---

[1] http://cijfers.hbo-raad.nl/index.htm.

[2] Van SQL-injectie is sprake bij (web)applicaties indien de invoer van gebruikers onvoldoende gecontroleerd wordt verwerkt in een SQL-statement. Indien een gebruiker op een invoerveld tekens invoert die ervoor zorgen dat een ongewenste query (vraag/selectie/bewerking) wordt uitgevoerd op de achterliggende database, is er sprake van een SQL-injectie. Om SQL-injectie te voorkomen, moet worden gedefinieerd welke tekens op een invoerveld zijn toegestaan en moet de invoer worden gevalideerd.

[3] XSS is de naam van een fout in de beveiliging van een webapplicatie. Het probleem wordt veroorzaakt doordat de invoer die de webapplicatie ontvangt (zoals cookie, URL, request parameters) niet afdoende wordt gevalideerd en hierdoor in de uitvoer terecht komt naar de eindgebruiker. Via deze bug in de website kan er kwaadaardige code (Jacascript, VBScript, ActiveX, HTML, Flash etc.) worden geïnjecteerd. Hiermee kunnen onder meer sessiecookies worden bekeken, een sessie van een gebruiker worden overgenomen, de functionaliteit van een website worden verrijkt of onbedoelde acties voor een gebruiker worden uitgevoerd.

Meer specifiek is het onderzoek toegespitst op het informatiesysteem X. In het informatiesysteem X worden - onder meer - rasgegevens van studenten verwerkt. Dit zijn bijzondere persoonsgegevens in de zin van artikel 16 Wbp.

2.3 Werkwijze

Bij brief van 2 april 2012 heeft het CBP de HAN verzocht om inlichtingen. Deze informatie is bij brief van 17 april 2012 verstrekt.

Op 28 juni 2012 hebben drie medewerkers van het CBP een onderzoek ter plaatse uitgevoerd bij de HAN, waarbij interviews zijn afgenomen met het hoofd ICT, een studieloopbaanbegeleider, twee functioneel beheerders en de functionaris voor de gegevensbescherming.

De HAN heeft nadere informatie verstrekt bij brieven van 29 juni 2012 en 2 juli 2012 en per e-mails van 2 juli 2012 en 17 juli 2012.

Per e-mail van 5 oktober 2012 heeft het CBP de HAN laten weten dat het verwacht het rapport van voorlopige bevindingen in november 2012 toe te sturen.

Het CBP heeft het rapport van voorlopige bevindingen bij brief van 16 november 2012 aan de HAN toegestuurd.

De HAN heeft het CBP per e-mail van 28 november 2012 verzocht om uitstel tot 6 december 2012 voor het geven van een schriftelijke reactie op het rapport van voorlopige bevindingen. Het CBP heeft dit verzoek per e-mail van gelijke datum toegewezen.

Bij brief van 4 december 2012 heeft de HAN gereageerd op het rapport van voorlopige bevindingen.

2.4 Algemeen juridisch kader

Ingevolge artikel 13 Wbp legt de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen de aantasting van gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan.[4] Voornoemde maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.[5]

[4] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98.
[5] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98.

Het CBP heeft de door de HAN getroffen maatregelen onderzocht ten aanzien van de volgende beveiligingsaspecten:

1. Informatiebeveiligingsbeleid;
2. Logische toegangsbeveiliging;
3. Cryptografische beheersmaatregelen;
4. Logging en controle;
5. Beheer van informatiebeveiligingsincidenten;
6. Audit informatiebeveiliging.

Bij de toetsing van deze beveiligingsmaatregelen aan artikel 13 Wbp is de Code voor Informatiebeveiliging als meetinstrument gebruikt. De Code voor Informatiebeveiliging is een technologie-neutrale standaard die binnen de informatiebeveiliging breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen. De Code voor Informatiebeveiliging is bovendien opgenomen op de 'pas toe of leg uit'-lijst van zowel het College als het Forum Standaardisatie. Dit betekent dat (semi-)overheidsorganisaties, waaronder onderwijsinstellingen, de Code voor Informatiebeveiliging toe moeten passen of uit moeten leggen waarom ze dat niet doen.

In hoofdstuk 2 van dit rapport zijn de bepalingen van de Code voor Informatiebeveiliging betreffende voornoemde beveiligingsmaatregelen nader uitgewerkt. Met die beveiligingsmaatregelen kan invulling worden gegeven aan artikel 13 Wbp.

3. BEVINDINGEN

3.1 Informatiebeveiligingsbeleid

3.1.1 Uitwerking juridisch kader

Norm 5.1 van de Code voor Informatiebeveiliging bepaalt dat de directie een informatiebeveiligingsbeleid voor de hele organisatie dient uit te brengen en te handhaven. Hiermee geeft de directie een duidelijke beleidsrichting aan in overeenstemming met de bedrijfsdoelstellingen en demonstreert de directie dat ze informatiebeveiliging ondersteunt en zich hiertoe verplicht.

Dit beveiligingsbeleid dient door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen (norm 5.1.1 van de Code voor Informatiebeveiliging).

Ingevolge norm 5.1.2 van de Code voor Informatiebeveiliging dient het informatiebeveiligingsbeleid voorts met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

3.1.2 Feitelijke bevindingen

Het informatiebeveiligingsbeleid van de HAN dateert van december 2011 en is bij besluit van het College van Bestuur van 3 april 2012 vastgesteld. Dit beleid geeft onder 'Bewustwording en training' aan dat regelmatig terugkerende bewustwordingscampagnes voor studenten, medewerkers en gasten onderdeel van het beleid zijn. Tevens is onder 'Organisatie van de informatiebeveiligingsfunctie' opgenomen dat iedere leidinggevende de taak heeft om ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid, om toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers, alsmede om periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen.

3.1.3 Beoordeling

De HAN beschikt over een recent informatiebeveiligingsbeleid dat is vastgesteld door het College van Bestuur. Dit beleid geeft aan dat informatiebeveiliging regelmatig onder de aandacht wordt gebracht van studenten, medewerkers en gasten. Daarmee voldoet de HAN aan voornoemde normen 5.1, 5.1.1 en 5.1.2 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

3.2 Logische toegangsbeveiliging

3.2.1 Uitwerking juridisch kader

I. Toegangsbeheersing

Ingevolge norm 11.1 van de Code voor Informatiebeveiliging dient de toegang tot informatie en IT-voorzieningen te worden beheerst. Hiertoe dienen er - onder meer - standaard gebruikersprofielen met toegangsrechten voor veelvoorkomende rollen in de organisatie te zijn (norm 11.1.1, sub f, van de Code voor Informatiebeveiliging) en dienen toegangsbeveiligingsrollen gescheiden te zijn, bijvoorbeeld ten aanzien van toegangsverzoek, toegangsautorisatie en toegangsadministratie (norm 11.1.1, sub h, van de Code voor Informatiebeveiliging).

II. Beheer van toegangsrechten van gebruikers

Norm 11.2 van de Code voor Informatiebeveiliging bepaalt dat er formele procedures dienen te zijn voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen en -diensten. In de procedures dienen alle fasen in de levenscyclus van gebruikerstoegang te worden vastgelegd, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben.

III. Blokkeren en aanpassen toegangsrechten

Norm 8.3.3 van de Code voor Informatiebeveiliging bepaalt dat de toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen dienen te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of na wijziging dient te worden aangepast.

IV. Beoordeling toegangsrechten

Ingevolge norm 11.2.4 van de Code voor Informatiebeveiliging dienen toegangsrechten van gebruikers regelmatig te worden beoordeeld in een formeel proces.

V. Gebruik van wachtwoorden

Uit norm 11.3 van de Code voor Informatiebeveiliging volgt dat gebruikers op de hoogte dienen te worden gebracht van hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden. Gebruikers dienen te worden geadviseerd over het kiezen en gebruiken van wachtwoorden overeenkomstig norm 11.3.1 van de Code voor Informatiebeveiliging.

VI. SQL-injectie en XSS

Artikel 13 Wbp vereist dat passende maatregelen moeten worden genomen om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking, waaronder onbevoegde kennisneming, wijziging, of verstrekking van gegevens. Ook ingevolge de Code voor Informatiebeveiliging (bijvoorbeeld norm 11.6) dient onbevoegde toegang tot informatie te worden voorkomen. Door middel van SQL-injectie en XSS kan onbevoegde toegang tot

informatie worden verkregen. Hiertegen dienen derhalve passende maatregelen te worden getroffen.

3.2.2 *Feitelijke bevindingen*

I. Toegangsbeheersing

Tijdens het onderzoek ter plaatse heeft de HAN verklaard dat binnen de applicaties met functiegroepen wordt gewerkt. Het document 'Overzicht functionaliteiten (rollen en rechten) in het informatiesysteem X' geeft de hoofd- en subrollen weer die aan medewerkers en studenten van de HAN worden toegekend alsmede de daarbij behorende rechten ten aanzien van het informatiesysteem X.

Gevraagd naar de verantwoordelijkheid voor en feitelijke toekenning van autorisaties heeft de HAN voorts geantwoord dat elk proces een eigenaar heeft die verantwoordelijk is voor het proces. De functioneel beheerder bepaalt wat je mag (autorisatie) en de ICT-afdeling zorgt voor de feitelijke uitvoering.

II. Beheer van toegangsrechten van gebruikers

Het document 'Procedure autorisaties' van 1 september 2011 beschrijft de procedure voor het toekennen van autorisaties voor het informatiesysteem X aan medewerkers en studenten van de HAN.

De rechten die onderwijskundig personeel van de HAN heeft ten aanzien van het informatiesysteem X zijn afhankelijk van de subrollen die aan dit personeel zijn toegekend. De procedure voor het toekennen van deze rolverdeling is nader uitgewerkt in het document 'Het toekennen van rollen aan onderwijskundig personeel'.

In het rapport van voorlopige bevindingen heeft het CBP geconcludeerd dat uit voornoemde documenten noch anderszins is gebleken dat de *wijziging* en *beëindiging* van de autorisaties en subrollen zijn belegd in een formele procedure. Daarmee voldeed de HAN *niet* aan norm 11.2 van de Code voor Informatiebeveiliging die voorschrijft dat *alle* fasen in de levenscyclus van gebruikerstoegang in een formele procedure dienen te worden vastgelegd. De HAN handelde derhalve op dit onderdeel in strijd met artikel 13 Wbp.

Naar aanleiding van het rapport van voorlopige bevindingen heeft de HAN de documenten 'Procedure autorisaties' (27 november 2012) en 'Handboek' (5 december) aangevuld met een beschrijving van de procedure voor het wijzigen en beëindigen van abonnementen en rollen.

III. Blokkeren en aanpassen toegangsrechten

De HAN heeft tijdens het onderzoek ter plaatse verklaard dat toegangsrechten van medewerkers en studenten van de HAN worden gewijzigd of beëindigd ingeval van een wijziging of beëindiging van het dienstverband of de studie.

IV. Beoordeling toegangsrechten

Het document 'Procedures autorisaties' vermeldt dat maandelijks de toegekende SZ+ (studentzaken) rechten worden gecheckt op actualiteit. Tevens

wordt periodiek (minimaal 1 keer per kwartaal) bekeken van welke medewerkers SZ de autorisatie moet worden ingetrokken.

In het rapport van voorlopige bevindingen heeft het CBP geconcludeerd dat uit voornoemd document noch anderszins is gebleken dat *tevens* de toegangsrechten van andere medewerkers of van studenten van de HAN regelmatig worden beoordeeld. Daarmee voldeed de HAN *niet* aan norm 11.2.4 van de Code voor Informatiebeveiliging. De HAN handelde derhalve op dit onderdeel in strijd met artikel 13 Wbp.

Naar aanleiding van het rapport van voorlopige bevindingen heeft de HAN het document 'Procedure autorisaties' (27 november 2012) aangevuld met een beschrijving van de wijze waarop de toegangsrechten van andere medewerkers van de HAN periodiek worden gecontroleerd. Voorts heeft de HAN aangevoerd dat het niet zinvol is om de toegangsrechten van studenten regelmatig te beoordelen, aangezien zij deze rechten alleen hebben voor zover zij student zijn bij de HAN. Bovendien kunnen studenten slechts hun eigen persoonsgegevens inzien en verliezen ze automatisch hun abonnement op en toegangsrechten tot het informatiesysteem X zodra hun studentschap eindigt.

V. Gebruik van wachtwoorden

De HAN hanteert het 'Wachtwoordbeleid Hogeschool van Arnhem en Nijmegen' van 25 augustus 2011. Dit beleid bepaalt dat alle gebruikers advies dienen te krijgen over - kort weergegeven - het kiezen, wijzigen en gebruiken van wachtwoorden.

VI. SQL-injectie en XSS

Per e-mail van 2 juli 2012 heeft de HAN aangegeven dat het jaarlijks een onderzoek doet naar kwetsbaarheden in alle servers, ook naar SQL-injectie en XSS. Bij constatering van kwetsbaarheden worden maatregelen genomen om misbruik te voorkomen. Tevens voert de HAN volgens voornoemde e-mail interne risicoanalyses uit op de belangrijkste systemen. Indien er behoefte is om een voorziening te controleren op kwetsbaarheden voor SQL-injecties of XSS, dan wordt dit meegenomen in het advies richting de eigenaar van de voorziening.

3.2.3 Beoordeling

I. Toegangsbeheersing

De functiegroepen (hoofd- en subrollen) met bijbehorende rechten ten aanzien van het informatiesysteem X betreft, overeenkomstig voornoemde norm 11.1.1, sub f, van de Code voor Informatiebeveiliging, de standaard gebruikersprofielen met toegangsrechten voor veelvoorkomende rollen in de organisatie.

De verantwoordelijkheid voor en feitelijke toekenning van autorisaties zijn voorts bij verschillende medewerkers van de HAN belegd. Er is derhalve sprake van een scheiding van toegangsbeveiligingsrollen zoals voorgeschreven in voornoemde norm 11.1.1, sub h, van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

II. Beheer van toegangsrechten van gebruikers

De documenten 'Gewijzigde Procedure Autorisaties' van 27 november 2012, 'Het toekennen van rollen aan onderwijskundig personeel' en 'Handboek' van 5 december beschrijven de procedures voor het toekennen, wijzigen en beëindigen van autorisaties, abonnementen en (sub)rollen. Daarmee voldoet de HAN aan norm 11.2 van de Code voor Informatiebeveiliging die voorschrijft dat alle fasen in de levenscyclus van gebruikerstoegang in een formele procedure dienen te worden vastgelegd.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* meer in strijd met artikel 13 Wbp handelt.

III. Blokkeren en aanpassen toegangsrechten

Toegangsrechten van medewerkers en studenten van de HAN worden gewijzigd of beëindigd ingeval van een wijziging of beëindiging van het dienstverband of de studie. Daarmee voldoet de HAN aan voornoemde norm 8.3.3 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

IV. Beoordeling toegangsrechten

Het document 'Gewijzigde Procedure Autorisaties' van 27 november 2012 beschrijft de wijze waarop toegangsrechten van alle medewerkers van de HAN periodiek worden gecontroleerd. Voorts heeft de HAN gemotiveerd aangegeven waarom hij het niet zinvol acht om de toegangsrechten van studenten regelmatig te beoordelen. Het CBP is het met dit oordeel van de HAN eens, gelet op het gegeven dat studenten alleen toegangsrechten tot het informatiesysteem X hebben voor zover zij student zijn bij de HAN, zij slechts hun eigen persoonsgegevens kunnen inzien en automatisch hun toegangsrechten tot het informatiesysteem X verliezen zodra hun studentschap eindigt. De HAN voldoet derhalve aan norm 11.2.4 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* meer in strijd met artikel 13 Wbp handelt.

V. Gebruik van wachtwoorden

De gebruikers dienen op grond van het wachtwoordbeleid van de HAN geadviseerd te worden over - kort weergegeven - het kiezen, wijzigen en gebruiken van wachtwoorden. Dit beleid komt overeen met voornoemde norm 11.3.1 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

VI. SQL-injectie en XSS

De HAN doet jaarlijks een onderzoek naar kwetsbaarheden in servers, waaronder SQL-injectie en XSS. Ingeval er kwetsbaarheden worden geconstateerd, neemt de HAN maatregelen om misbruik te voorkomen. Tevens wordt in het kader van de interne risicoanalyse de eigenaar van een voorziening geadviseerd over de controle op kwetsbaarheden voor SQL-injecties of XSS indien daartoe behoefte is. Hiermee heeft de HAN maatregelen getroffen om onbevoegde toegang tot het informatiesysteem X middels SQL-injectie en XSS te voorkomen.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

3.3 Cryptografische beheersmaatregelen

3.3.1 Uitwerking juridisch kader

De vertrouwelijkheid, authenticiteit en integriteit van informatie dient te worden beschermd met behulp van cryptografische maatregelen (norm 12.3 van de Code voor Informatiebeveiliging). Cryptografische maatregelen dienen onder meer te worden toegepast bij verzending van persoonsgegevens via het internet en bij opslag van persoonsgegevens in gegevensverzamelingen die via het internet kunnen worden benaderd.

3.3.2 Feitelijke bevindingen

Per e-mail van 2 juli 2012 heeft de HAN aangegeven dat bij transport van persoonsgegevens zoveel mogelijk gebruik wordt gemaakt van versleuteling via https. Het draadloze netwerk Y wordt versleuteld via V. Daarnaast maakt de HAN volgens voornoemde e-mail voor een deel van het draadloze netwerk nog gebruik van het dynamisch W protocol. Dit wordt evenwel uitgefaseerd vanwege de overstap naar het netwerk Y.

3.3.3 Beoordeling

De HAN heeft, overeenkomstig voornoemde norm 12.3 van de Code voor Informatiebeveiliging, cryptografische maatregelen getroffen ten aanzien van transport van persoonsgegevens en het draadloze netwerk.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

3.4 Logging en controle

3.4.1 Uitwerking juridisch kader

Norm 10.10 van de Code voor Informatiebeveiliging bepaalt dat systemen dienen te worden gecontroleerd en informatiebeveiligingsgebeurtenissen dienen te worden geregistreerd om onbevoegde informatieverwerkingsactiviteiten te ontdekken. Hiertoe dienen activiteiten van gebruikers te worden vastgelegd in audit-logbestanden (norm 10.10.1 van de Code voor Informatiebeveiliging). Deze logbestanden dienen ingevolge norm 10.10.2 van de Code voor Informatiebeveiliging regelmatig te worden beoordeeld.

3.4.2 Feitelijke bevindingen

De HAN heeft tijdens het onderzoek ter plaatse verklaard dat de toegang tot persoonsgegevens in het informatiesysteem X wordt gelogd. De logfiles worden niet periodiek gecontroleerd (steekproeven), maar alleen in geval van incidenten.

In de reactie op de voorlopige bevindingen heeft de HAN aangegeven dat de genoemde logging niet geschikt is om een ongeoorloofde toegang op te merken. Tevens heeft de HAN aangegeven dat inloggen in het informatiesysteem X plaatsvindt middels single sign on (SSO). Een mislukte inlogpoging wordt daarom niet opgemerkt in het informatiesysteem X, maar in de applicatie voor SSO. In de huidige SSO-applicatie wordt gelogd, maar is niet te zien op welke applicatie een mislukte inlogpoging betrekking heeft, aldus de HAN. De HAN is voornemens om voor 1 april 2013 over te gaan op een nieuw SSO-systeem, waarbij wel zichtbaar is op welke applicatie een mislukte inlogpoging betrekking heeft. Dan zal ook de logging maandelijks worden beoordeeld.

3.4.3 Beoordeling

De logfiles kunnen - thans - niet effectief worden ingezet om onbevoegde toegang te detecteren en worden - thans - niet regelmatig beoordeeld, zoals voorgeschreven door norm 10.10.2 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel handelt in strijd met artikel 13 Wbp.

3.5 Beheer van informatiebeveiligingsincidenten

3.5.1 Uitwerking juridisch kader

Norm 13.1 van de Code voor Informatiebeveiliging bepaalt dat er formele procedures voor rapportage van informatiebeveiligingsgebeurtenissen en escalatie dienen te zijn. Hierdoor kan worden bewerkstelligd dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met

informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Tevens dienen er ingevolge norm 13.2 van de Code voor Informatiebeveiliging verantwoordelijkheden en procedures te zijn voor het doeltreffend behandelen van informatiebeveiligingsgebeurtenissen en zwakke plekken, zodra ze zijn gerapporteerd. Hierdoor kan worden bewerkstelligd dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

3.5.2 Feitelijke bevindingen

Gevraagd naar de omgang met beveiligingsincidenten is tijdens het onderzoek ter plaatse geantwoord dat beveiligingsincidenten worden gemeld bij het Computer Emergency Response Team van de HAN (HAN-CERT). Het HAN-CERT is verantwoordelijk voor de coördinatie van het afhandelen van beveiligingsincidenten. Deze verantwoordelijkheden zijn opgenomen in het informatiebeveiligingsbeleid van de HAN.

De documenten 'ICT-reglement voor medewerkers van de Hogeschool van Arnhem en Nijmegen' van 26 mei 2010 en 'Studentenstatuut' van 22 juni 2012 beschrijven de procedure voor melding en afhandeling van incidenten.

Het HAN-CERT houdt een registratie van beveiligingsincidenten en getroffen maatregelen bij. De HAN heeft deze registratie van de jaren 2011 en 2012 overgelegd. Tijdens het onderzoek ter plaatse heeft de HAN voorts medegedeeld dat jaarlijks aan de stuurgroep informatiebeleid wordt gerapporteerd over incidenten en de afhandeling.

3.5.3 Beoordeling

De HAN beschikt over een procedure voor het melden en afhandelen van beveiligingsincidenten. Het HAN-CERT is verantwoordelijk voor de coördinatie van het afhandelen van de incidenten. Daarmee voldoet de HAN aan voornoemde normen 13.1 en 13.2 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

3.6 Audit informatiebeveiliging

3.6.1 Uitwerking juridisch kader

Informatiebeveiliging dient in een organisatie te worden geïmplementeerd en te worden beheerst (norm 6.1 van de Code voor Informatiebeveiliging). Ingevolge norm 6.1.8 van de Code voor Informatiebeveiliging dienen de benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan met geplande tussenpozen, of zodra zich significante

wijzigingen voordoen in de implementatie van de beveiliging, te worden beoordeeld. Dit betreft een zogenoemde informatiebeveiligingsaudit. Een dergelijke beoordeling is nodig om te waarborgen dat de organisatie een geschikte, toereikende en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert.

De beoordeling dient te worden uitgevoerd door personen die onafhankelijk zijn ten opzichte van de omgeving die wordt beoordeeld, bijvoorbeeld een interne auditor, een onafhankelijke manager of een derde partij die hierin is gespecialiseerd. De resultaten van de beoordeling dienen te worden vastgelegd en aan de directie te worden gerapporteerd.

3.6.2 Feitelijke bevindingen

Het informatiebeveiligingsbeleid van de HAN van december 2011 gaf aan dat er periodieke controles/audits door het HAN-CERT worden uitgevoerd. Tijdens het onderzoek ter plaatse heeft de HAN verklaard dat er controles plaatsvinden door de functionaris voor de gegevensbescherming, het HAN-CERT en de security manager ICT. Dit mag volgens de HAN evenwel geen audit heten, aangezien de controles minder formeel zijn en nog in de kinderschoenen staan. Uit het concept document 'Vragenlijst identificatie, classificatie en risicoanalyse HAN informatievoorzieningen' blijkt eveneens dat er ten aanzien van het informatiesysteem X geen audits zijn uitgevoerd.

In het rapport voorlopige bevindingen heeft het CBP geconcludeerd dat de HAN weliswaar periodieke controles uitvoert ten aanzien van het informatiesysteem X, maar dit geen onafhankelijke informatiebeveiligingsaudits in de zin van norm 6.1.8 van de Code voor Informatiebeveiliging betreffen. De HAN handelde derhalve op dit onderdeel in strijd met artikel 13 Wbp.

Naar aanleiding van het rapport van voorlopige bevindingen heeft de HAN zijn informatiebeveiligingsbeleid (november 2012) aangevuld, waardoor de verantwoordelijkheid voor de uitvoering van een informatiebeveiligingsaudit formeel is belegd bij de Information Security Officer. Tevens heeft de HAN op 8 januari 2013 telefonisch toegelicht dat het de eerdergenoemde controles geen 'informatiebeveiligingsaudit' noemde, maar een 'beveiligingsscan'. Bij nader inzien kunnen deze controles volgens de HAN echter wel worden aangemerkt als een informatiebeveiligingsaudit. Voorts heeft de HAN aangegeven dat in het concept document 'Vragenlijst identificatie, classificatie en risicoanalyse HAN informatievoorzieningen' staat dat er ten aanzien van het informatiesysteem X geen audits zijn uitgevoerd, aangezien de informatiebeveiligingsaudit voor het eerst werd uitgevoerd. Inmiddels is de audit afgerond en zal het worden herhaald.

3.6.3 Beoordeling

De HAN heeft - inmiddels - een informatiebeveiligingsaudit uitgevoerd. Het gewijzigde informatiebeveiligingsbeleid van november 2012 vermeldt dat de

bedrijfskritische informatiesystemen van de HAN tenminste eens per twee jaar intern worden geaudit. Indien een informatiesysteem wordt vervangen of indien zich significante wijzigingen voordoen in de implementatie van de beveiliging wordt volgens het informatiebeveiligingsbeleid op dat moment een audit uitgevoerd. Voorts heeft de HAN de verantwoordelijkheid voor de uitvoering van de interne informatiebeveiligingsaudits formeel belegd bij de Information Security Officer, die onafhankelijk staat ten opzichte van de omgeving die wordt beoordeeld.

Het CBP concludeert aldus dat de HAN op dit onderdeel *niet* meer in strijd met artikel 13 Wbp handelt.

4. CONCLUSIE

Het CBP heeft onderzocht of de HAN voldoende passende technische en organisatorische maatregelen heeft getroffen teneinde persoonsgegevens van studenten in het informatiesysteem X te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (artikel 13 Wbp). Naar aanleiding van dit onderzoek concludeert het CBP als volgt:

Geen overtreding
Er is *geen* sprake van een overtreding van artikel 13 Wbp ten aanzien van de volgende informatiebeveiligingsaspecten:

- Informatiebeveiligingsbeleid (zie paragraaf 3.1)
- Toegangsbeheersing (zie paragraaf 3.2, sub I)
- Beheer van toegangsrechten van gebruikers (zie paragraaf 3.2, sub II)
- Blokkeren en aanpassen toegangsrechten (zie paragraaf 3.2, sub III)
- Beoordeling toegangsrechten (zie paragraaf 3.2, sub IV)
- Gebruik van wachtwoorden (zie paragraaf 3.2, sub V)
- SQL-injectie en XSS (zie paragraaf 3.2, sub VI)
- Crytografische beheersmaatregelen (zie paragraaf 3.3)
- Beheer van informatiebeveiligingsincidenten (zie paragraaf 3.5)
- Audit informatiebeveiliging (zie paragraaf 3.6)

Overtreding
Er is *wel* sprake van een overtreding van artikel 13 Wbp ten aanzien van de volgende informatiebeveiligingsaspecten:

- Logging en controle (zie paragraaf 3.4)