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 Utrecht

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 Utrecht (hierna: de HU) 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 A. In het informatiesysteem A worden - onder meer - gezondheidsgegevens en rasgegevens van studenten verwerkt. Dit zijn bijzondere persoonsgegevens in de zin van artikel 16 Wbp.

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

Het CBP constateert dat de HU onvoldoende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten 'Informatiebeveiligingsbeleid', 'Beoordeling toegangsrechten', 'SQL-injectie en Cross-Site Scripting (XSS)' en 'Logging en controle'. De HU handelt hierdoor in strijd met artikel 13 Wbp.

Ten aanzien van de onderzochte beveiligingsaspecten 'Toegangsbeheersing', 'Beheer van toegangsrechten van gebruikers', 'Blokkeren en aanpassen van toegangsrechten', 'Gebruik van wachtwoorden', 'Cryptografische beheersmaatregelen', 'Beheer van informatiebeveiligingsincidenten' en 'Audit informatiebeveiliging' constateert het CBP geen overtredingen.

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 HU in 2011 37.481 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 HU verwerkt persoonsgegevens van studenten op zijn interne informatiesystemen. Het onderzoek beoogt vast te stellen of de HU 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 A. In het informatiesysteem A worden - onder meer - gezondheidsgegevens en 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 HU verzocht om inlichtingen. Deze informatie is bij brief van 18 april 2012 verstrekt.

Op 22 juni 2012 hebben drie medewerkers van het CBP een onderzoek ter plaatse uitgevoerd bij de HU, waarbij interviews zijn afgenomen met de Chief Information Officer, de Security Officer en de (voormalig) functioneel beheerder van het informatiesysteem A.

Op 11 juli 2012 heeft een tweede onderzoek ter plaatse plaatsgevonden. Tijdens dit onderzoek hebben drie medewerkers van het CBP gesproken met de Security Officer, een docent-tevens studieloopbaanbegeleider en een decaan.

De HU heeft nadere informatie verstrekt bij brieven van 14 mei 2012 en 19 juli 2012 en per e-mail van 15 augustus 2012.

Per e-mail van 5 oktober 2012 heeft het CBP de HU 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 HU toegestuurd.

De HU heeft het CBP per e-mail van 21 november 2012 verzocht om uitstel tot 8 december 2012 voor het geven van een schriftelijke reactie op het rapport van voorlopige bevindingen. Het CBP heeft dit verzoek per e-mail van 22 november 2012 toegewezen.

Bij brief van 7 december 2012 heeft de HU 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

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

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]

Het CBP heeft de door HU 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.

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

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 vastgestelde informatiebeveiligingsbeleid van de HU dateert van 12 juni 2001. Dit beleid geeft onder 'Beleidsuitgangspunten' aan dat de zorg voor de beveiliging van gegevens een verantwoordelijkheid is van alle medewerkers en dat beveiligingsbewustzijn hierbij van essentieel belang is.

Bij brief van 18 april 2012 en tijdens het eerste onderzoek ter plaatse heeft de HU aangegeven dat het huidige beleidsdocument zal worden vervangen. De HU heeft het concept informatiebeveiligingsbeleid gedateerd 24 april 2012 overgelegd.

In de reactie op de voorlopige bevindingen heeft de HU aangegeven te erkennen dat het informatiebeveiligingsbeleid gedateerd is. De herziening van dit beleid is volgens de HU evenwel in volle gang.

3.1.3 Beoordeling

Het huidige informatiebeveiligingsbeleid van de HU dateert van juni 2001. Dit beleid zal worden herzien. Het beleidsdocument van 24 april 2012 betreft evenwel nog een concept. De HU beschikt derhalve niet over een geschikt, toereikend en doeltreffend informatiebeveiligingsbeleid. Daarmee voldoet de HU niet aan norm 5.1.2 van de Code voor Informatiebeveiliging.

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

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 eerste onderzoek ter plaatse heeft de HU verklaard dat het informatiesysteem A verschillende functiegroepen kent op basis waarvan wordt bepaald welke rol en bevoegdheden iemand in het informatiesysteem A heeft. Het document 'Beschrijving Beheerprocessen Functioneel Beheer Hogeschool Utrecht' van 25 mei 2011 geeft de rollen, taken en bevoegdheden weer van medewerkers in beheersprocessen.

Dit document noemt voorts de volgende taken van medewerkers van de HU ten aanzien van autorisaties:

- De Functioneel Beheerder bewaakt de gebruikersprofielen en autorisaties;
- De Helpdesk neemt autorisatieverzoeken in behandeling;
- De Technisch Applicatie Beheerder wikkelt autorisatieverzoeken af.

De in dit document beschreven procedures voor het aanvragen, toekennen en wijzigen en voor het afmelden van accounts en rechten voor informatiesystemen concretiseren deze taken nader. Tevens blijkt uit deze procedures dat de Afdelingsmanager een account voor gebruikers aanvraagt alsmede een uitdiensttreding of functiewijziging meldt.

II. Beheer van toegangsrechten van gebruikers

Het document 'Beschrijving Beheerprocessen Functioneel Beheer Hogeschool Utrecht' beschrijft de procedure voor het aanvragen en toekennen van accounts en rechten voor informatiesystemen van de HU. Deze procedure is ook van toepassing op een wijziging van een account of accountrechten. Tevens beschrijft dit document de procedure voor afmelding van gebruikersaccounts en rechten.

III. Blokkeren en aanpassen toegangsrechten

De HU heeft tijdens het eerste onderzoek ter plaatse verklaard dat accounts van medewerkers en studenten van de HU worden aangepast of afgesloten ingeval van een wijziging of beëindiging van het dienstverband of de studie.

IV. Beoordeling toegangsrechten

Het document 'Beschrijving Beheerprocessen Functioneel Beheer Hogeschool Utrecht' beschrijft het proces van een jaarlijkse controle op de rechten van gebruikers in een informatiesysteem. De HU heeft op 7 augustus 2012 evenwel telefonisch verklaard dat deze controle met betrekking tot het informatiesysteem A de afgelopen twee à drie jaar niet is uitgevoerd.

V. Gebruik van wachtwoorden

Het document 'Gedragsregels ICT HU' van 3 april 2006 bevat voorschriften omtrent - kort weergegeven - het kiezen, wijzigen en gebruiken van

wachtwoorden. Tevens wordt een gebruiker van de HU een aantal regels omtrent het kiezen en wijzigen van een wachtwoord getoond op het beeldscherm van de computer ingeval hij zijn wachtwoord wil wijzigen. Een screenshot 'wachtwoord wijzigen' met deze regels is overgelegd.

VI. SQL-injectie en XSS

De HU heeft tijdens het tweede onderzoek ter plaatse verklaard dat er gebruik wordt gemaakt van een B-systeem op de servers, waaronder de server A. Hierbij wordt volgens de HU "een soort SQL-injectie op de systemen geprobeerd".

In reactie op het rapport van voorlopige bevindingen heeft de HU nader toegelicht dat voor het informatiesysteem A geen gebruik wordt gemaakt van het B-systeem daar waar het betreft de controle op SQL-injectie en XSS kwetsbaarheden. Volgens de HU wordt door het inzetten van het B-systeem evenwel een bredere set aan maatregelen getroffen ter controle van onbevoegde toegang. Bovendien zou uit niets zijn gebleken dat het informatiesysteem A in de praktijk kwetsbaar is voor SQL-injectie en XSS aanvallen. Desondanks is de HU voornemens om nogmaals de analyse te maken of regelmatige SQL-injectie en XSS controles door het B-systeem verder ingezet kunnen worden met betrekking tot het informatiesysteem A.

3.2.3 Beoordeling

I. Toegangsbeheersing

De functiegroepen met bijbehorende rollen en bevoegdheden ten aanzien van het informatiesysteem A betreffen, 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 aanvraag, het in behandeling nemen en het afwikkelen van autorisaties zijn voorts bij verschillende medewerkers van de HU 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 HU op dit onderdeel *niet* in strijd met artikel 13 Wbp handelt.

II. Beheer van toegangsrechten van gebruikers

Het document 'Beschrijving Beheerprocessen Functioneel Beheer Hogeschool Utrecht' beschrijft de procedure voor zowel het aanvragen, toekennen en wijzigen, als het afmelden van accounts en rechten voor informatiesystemen van de HU. Daarmee voldoet de HU aan voornoemde norm 11.2 van de Code voor Informatiebeveiliging die voorschrijft dat alle fasen in de levenscyclus van gebruikerstoegang in een formele procedure behoren te worden vastgelegd.

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

III. Blokkeren en aanpassen toegangsrechten
Toegangsrechten van medewerkers en studenten van de HU worden aangepast of afgesloten ingeval van een wijziging of beëindiging van het dienstverband of de studie. Daarmee voldoet de HU aan voornoemde norm 8.3.3 van de Code voor Informatiebeveiliging.

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

IV. Beoordeling toegangsrechten
De HU heeft de afgelopen jaren geen controle uitgevoerd op de rechten van gebruikers met betrekking tot het informatiesysteem A. Daarmee voldoet de HU *niet* aan norm 11.2.4 van de Code voor Informatiebeveiliging.

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

V. Gebruik van wachtwoorden
Voorschriften omtrent - kort weergegeven - het kiezen, wijzigen en gebruiken van wachtwoorden zijn neergelegd in het document 'Gedragsregels ICT HU' en worden tevens getoond ingeval een gebruiker zijn wachtwoord wil wijzigen. Daarmee voldoet de HU aan norm 11.3.1 van de Code voor Informatiebeveiliging.

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

VI. SQL-injectie en XSS
Weliswaar heeft de HU maatregelen getroffen ter controle van diverse mogelijkheden van onbevoegde toegang tot het informatiesysteem A, doch niet specifiek ten aanzien van SQL-injectie en XSS.

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

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

Tijdens het eerste onderzoek ter plaatse heeft de HU verklaard dat de studielinkverbinding, backoffice-applicaties en webapplicaties gebruik maken van https. De draadloze verbindingen zijn beveiligd door middel van C authenticatie en zijn encrypted.

3.3.3 Beoordeling

De HU heeft, overeenkomstig voornoemde norm 12.3 van de Code voor Informatiebeveiliging, cryptografische maatregelen getroffen ten aanzien van de studielinkverbinding, backoffice-applicaties, webapplicaties en de draadloze verbindingen.

Het CBP concludeert aldus dat de HU 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

Op de vraag of de toegang tot persoonsgegevens wordt gelogd heeft de HU tijdens het eerste onderzoek ter plaatse geantwoord dat het informatiesysteem A een eigen logging heeft. De logfiles worden niet actief handmatig gecontroleerd. De HU beschikt wel over een monitorsysteem, waardoor reactief gecontroleerd kan worden. Ingeval van een vermoeden van ongeoorloofde toegang, is het derhalve mogelijk om dit in de back-up van de logfiles na te zoeken.

In de reactie op de voorlopige bevindingen heeft de HU aangegeven dat het voornemens is om het ondernemen van acties ter verbetering van de controleprocedures op de logging op te nemen in het securityjaarplan voor 2013.

3.4.3 Beoordeling

De toegang tot persoonsgegevens in het informatiesysteem A wordt gelogd overeenkomstig voornoemde norm 10.10.1 van de Code voor

Informatiebeveiliging. Deze logfiles worden - thans - evenwel niet regelmatig beoordeeld, zoals voorgeschreven door norm 10.10.2 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HU 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

Het document 'Beschrijving Beheersprocessen Functioneel Beheer Hogeschool Utrecht' beschrijft de procedure van de verantwoordelijkheden en activiteiten voor het registeren en behandelen van incidenten alsmede de terugkoppeling en registratie van het resultaat.

Voorts heeft de HU tijdens het eerste onderzoek ter plaatse verklaard dat een (virtueel) logboek wordt bijgehouden van beveiligingsincidenten. De HU heeft de resultaten uit dit logboek van januari 2012 tot en met juni 2012 overgelegd.

3.5.3 Beoordeling

De HU beschikt over een procedure met daarin de verantwoordelijkheden en activiteiten voor het registeren en behandelen van incidenten alsmede de terugkoppeling en registratie van het resultaat. Daarmee voldoet de HU aan voornoemde normen 13.1 en 13.2 van de Code voor Informatiebeveiliging.

Het CBP concludeert aldus dat de HU 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 zogenoemd 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

Tijdens het eerste onderzoek ter plaatse en in de reactie op het rapport van voorlopige bevindingen heeft de HU aangegeven dat er een informatiebeveiligingsaudit wordt uitgevoerd door een externe auditor als onderdeel van de jaarrekeningcontrole. Tevens heeft de HU deelgenomen aan de pilot van de op ISO27002 gebaseerde D-audit. Deze D-audit gaat volgends de HU jaarlijks op het informatiesysteem A plaatsvinden en wordt uitgevoerd door de Security Officer van de HU.

3.6.3 Beoordeling

De HU laat jaarlijks een informatiesysteemaudit, als onderdeel van de jaarrekeningcontrole, uitvoeren en heeft deelgenomen aan de pilot van de D-audit. Deze D-audit zal jaarlijks worden herhaald. Beide audits worden uitgevoerd door personen die onafhankelijk zijn ten opzichte van de omgeving die is beoordeeld.

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

4. CONCLUSIE

Het CBP heeft onderzocht of de HU voldoende passende technische en organisatorische maatregelen heeft getroffen teneinde persoonsgegevens van studenten in het informatiesysteem A 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:

- 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)
- Gebruik van wachtwoorden (zie paragraaf 3.2, sub V)
- 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:

- Informatiebeveiligingsbeleid (zie paragraaf 3.1)
- Beoordeling toegangsrechten (zie paragraaf 3.2, sub IV)
- SQL-injectie en XSS (zie paragraaf 3.2, sub VI)
- Logging en controle (zie paragraaf 3.4)