UNIVERSITEIT TWENTE.

Leden van de Universiteitsraad
Secretariaat
Mevr. L. Tijink
Spiegel SP 438

COLLEGE VAN BESTUUR

DATUM
06-02-2013
ONS KENMERK
399.532
UW KENMERK
UR-12-182

ONDERWERP
Reactie op UR 12-182 inzake Lek ICT -systemen

Geachte leden van de Universiteitsraad,

In reactie op de vragen die door uw raad zijn gesteld in uw schrijven (kenmerk: UR 12-182), inzake: Lek ICT-systeem, kan ik u als volgt berichten.

Vooraf schets ik graag enige achtergrondinformatie.

Het systeem genoemd in het artikel in het UT-nieuws is de leenmodule van het OCLC-LBS-systeem. Dit is een systeem dat draait bij de dienst Bibliotheek & Archief (B&A) en dat ten behoeve van authenticatie informatie verkrijgt uit andere systemen (Osiris, HRM) door het inlezen van bestanden.
Medewerkers en studenten krijgen automatisch een toegangsnaam en een wachtwoord toegekend voor dit systeem.
Informatie van de medewerkers wordt door HR wekelijks aangeleverd en betreft de naam en het e-mailadres. Er worden geen adresgegevens van medewerkers geregistreerd.
Voor studenten wordt de relevante informatie wekelijks ontleend aan Osiris. Naast studentnaam en e-mailadres worden ook adresgegevens meegestuurd. Deze adresgegevens zijn noodzakelijk om tweede rappels te kunnen sturen als de leentermijn van boeken verstreken is.
In de praktijk blijkt dat veel medewerkers en studenten niet (meer) weten dat zij een account hebben in het uitleensysteem, waardoor ze hun initiële wachtwoord niet wijzigen.

B&A is op de hoogte van het feit dat de standaard routine voor het genereren van wachtwoorden van de leenmodule niet voldoet aan de eisen van deze tijd. De beste oplossing die de leverancier van het systeem biedt om het beveiligingsniveau te verhogen vergt verzenden van een random gegenereerd wachtwoord per e-mail. Bij de leverancier staat een verzoek uit de module geschikt te maken voor Single-Sign-On via LDAP.

Het probleem
Een student heeft gemeld dat het mogelijk is om adresgegevens via het systeem te achterhalen en heeft hierover, omdat een oplossing uitbleef, de publiciteit (UT-nieuws) gezocht. Als bewijs

heeft de student een bestand opgebouwd met adresgegevens afkomstig uit de leenmodule. Hierbij moet gebruik zijn gemaakt van studentnummers en studentnamen die aan andere systemen zijn ontleend waarin die vermeld staan. Met zoekfuncties in bijvoorbeeld het adresboek van de UT-mail, zijn alle studenten en hun studentnummers te achterhalen

De uitgevoerde actie
Vanwege de publiciteit is na overleg met de leverancier ervoor gekozen toch de actie uit te voeren waarbij het standaard wachtwoord wordt vervangen door een random wachtwoord dat per email naar de medewerkers en studenten wordt verstuurd. Hiermee werd beoogd het acute risico van hack-activiteiten weg te nemen. Door de tijdsdruk is dit helaas te haastig en onzorgvuldig uitgevoerd, waardoor de actie herhaald moest worden.
Bij de eerste poging is het Security-team van de UT (CERT-UT) onvoldoende geïnformeerd. De dienstdoende beheerder heeft de mailing afgebroken, omdat hij de e-mail heeft geïnterpreteerd als phishing-mail en aannam dat de bibliotheekserver (in de late avonduren) met de inlogpagina gekraakt was.

Antwoorden op de vragen van de Universiteitsraad:

Vraag 1: Was het college voor het verschijnen van dit artikel op de hoogte van het bestaan van dit lek? Zo nee, waarom niet?
Antwoord:
Nee, het college was niet op de hoogte van het potentiële risico.

Vraag 2: Het lek was al geruime tijd bekend, maar is in korte tijd verholpen. Kan het college verklaren, waarom dit lek toch zolang is blijven bestaan?
Antwoord:
Met maatregelen is gewacht, omdat in het overleg met de leverancier nog werd afgewacht of de gewenste oplossing, koppeling met LDAP, gerealiseerd kon worden. Na de publiciteit is er alsnog voor gekozen de al bestaande oplossing van de leverancier uit te voeren.

Vraag 3: Waarom is er gekozen voor een niet-permanente oplossing, die door een groot deel van de URaadsleden ook nog eens is opgevat als een phishingpoging?.
Antwoord:
De gekozen oplossing is wel permanent, maar verdient niet de schoonheidsprijs: wachtwoord in e-mail, risico dat e-mail opgevat wordt als phishing. Het is echter niet de door B&A gewenste oplossing, omdat de leverancier geen koppeling met LDAP kan bieden. Het meest ideale zou zijn gebruik maken van de Single-Sign-On-voorzieningen van de UT. Het OCLC-LBS-systeem is verouderd en staat op de nominatie om te worden vervangen. Sterke authenticatie en autorisatie is één van de voorwaarden die aan het nieuwe systeem gesteld gaat worden.

Vraag 4: welke stappen worden er ondernomen om dergelijke situaties in de toekomst te voorkomen?
Antwoord:
Periodiek vinden er UT-breed audits plaats, die onder meer door Operational Audit worden uitgevoerd. Hierbij wordt ook gekeken naar de informatiebeveiliging van systemen. Verder heeft UIM een (informatiebeveiliging)beleid ontwikkeld, waaraan de UT zich moet houden. Hierbij vindt er een classificatie van systemen plaats, waarbij naar het belang van het betreffend systeem voor de universiteit wordt gekeken. Aan de waarde van de classificatie zijn specifieke maatregelen gekoppeld.
De UT heeft een securityteam (CERT-UT) dat voor zover mogelijk 24/7 snel en adequaat op problemen reageert.

Vraag 5: Deelt het college de mening dat een gedegen IT-infrastructuur en bijbehorende beveiliging een organisatie als de UT past.
Antwoord:
Ja, die mening deelt het college.

Vraag 6: Welke stappen gaat het college ondernemen om deze situatie te verbeteren?
Antwoord:
Het college ziet toe op het uitvoeren van het vastgestelde Informatiebeveiligingsbeleid. Het college beseft dat er geen 100% beveiliging mogelijk is en streeft naar een hoge graad van beveiliging, waarbij het aspect van openheid in het gebruik van de infrastructuur niet uit het oog wordt verloren.
In het kader van het beleid worden maatregelen getroffen en activiteiten ondernomen om de veiligheid op niveau te brengen en te houden.

De UR heeft aanvullend tijdens het overleg op 7 november 2012 geconstateerd dat het via de exchange-server mogelijk is om s- en m-nummers te koppelen aan namen van respectievelijk. studenten en medewerkers. In reactie hierop kan ik u melden dat deze constatering klopt. In het verleden is een keuze gemaakt voor het inloggen op basis van een naam in plaats van een nummer vanuit persoonlijkheids-perspectief. Het veranderen van deze methodiek heeft impact op meer dan alleen de Exchange-omgeving. ICTS is opdracht gegeven om met een voorstel te komen dit punt op te lossen, daarbij rekening houdend met een impact analyse en een kosten/batenanalyse.

In het vertrouwen u hiermee namens het College van Bestuur voldoende geïnformeerd te hebben,

Met vriendelijke groet,

Mr. H.J. van Keulen
Secretaris van de Universiteit