Universitair Informatiemanagement

UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/14/0131/khv
Datum: 9 juni 2015

Wachtwoordbeleid Universiteit Twente

Inhoud

Samenvatting

Bij de opstelling van de Beleidsregels Identitymanagement Universiteit Twente[1] is ervoor gekozen om een apart wachtwoordbeleid op te stellen waarin alle aspecten opnieuw worden afgewogen en uitgewerkt. De verschillende inzichten worden in dit document belicht. Beveiligingsargumenten, gebruikerservaring en wetenschappelijke bevindingen komen aan de orde. Dit is bij de faculteiten, informatiebeveiligingswetenschappers en de security managers van ICTS getoetst.

In de Gedragscode ICT- en Internetgebruik[2] staat beschreven dat gebruikers hun wachtwoord geheim moeten houden. Veel verschillende adviezen over wachtwoordgebruik doen de ronde. De waarde van het UT-wachtwoord wordt geanalyseerd en de bedreigingen worden in kaart gebracht. Geconcludeerd wordt dat de waarde van het wijzigen van wachtwoorden zonder aanleiding erg twijfelachtig is.

De verplichting aan gebruikers om het wachtwoord eens per jaar te wijzigen vervalt niet. Wanneer er aanwijzingen zijn dat hun wachtwoord is gecompromitteerd dan dienen gebruikers het advies te krijgen dit te wijzigen. De uitspraken in de Beleidsregels Identitymanagement Universiteit Twente over wachtwoorden worden overeenkomstig aangepast.

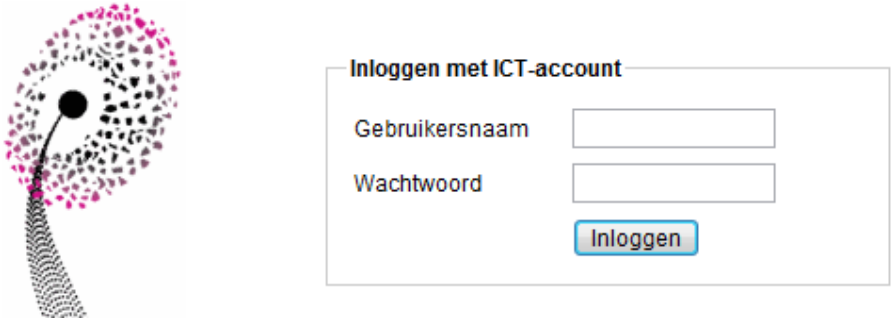
Voorlichting over de waarde van wachtwoorden, de noodzaak deze vertrouwelijk te houden en het UT-wachtwoord niet elders te gebruiken moet bij de UT worden geïntensiveerd. Voor het geauthenticeerd gebruik van externe websites wordt zo veel mogelijk gebruik gemaakt van SURFconext, voor andere websites zijn gebruikers zelf verantwoordelijk voor hun gebruikersnaam/wachtwoord. Er kan meer voorlichting gegeven worden hoe hier verantwoord mee om te gaan, bijvoorbeeld door het gebruik van een wachtwoordkluis.

Op termijn zal de UT gebruik maken van multifactorauthenticatie, bijvoorbeeld middels tokens of SMS. Dit zal gebeuren op basis van vastgestelde betrouwbaarheidsniveaus. De UT volgt hierbij de ontwikkelingen bij SURFnet.

[1] Beleidsregels Identitymanagement Universiteit Twente, kenmerk SB/UIM/13/0213/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf
[2] Gedragscode ICT- en Internetgebruik Universiteit Twente 2009, zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_ict_mw-nl.pdf

1 Inleiding

Om te voorkomen dat iedereen toegang tot vertrouwelijke informatie kan krijgen en om te voorkomen dat informatie door onbevoegden gewijzigd kan worden, identificeren medewerkers op de Universiteit Twente zich met een gebruikersnaam en authenticeren zich vervolgens met een wachtwoord.



Gebruikers houden niet van wachtwoorden en negeren dan ook regelmatig diverse beveiligingsadviezen. Afgedwongen maatregelen als het periodiek wijzigen worden als irritant en overbodig ervaren. Bij de opstelling van de Beleidsregels Identitymanagement Universiteit Twente[3] is er daarom voor gekozen om een apart wachtwoordbeleid op te stellen waarin alle aspecten opnieuw worden afgewogen en uitgewerkt. Dit document vervult deze rol door een gedachteproces te beschrijven. Een dergelijke uitvoerige methode is noodzakelijk omdat er op de UT meerdere tegengestelde meningen zijn geuit over dit onderwerp en alleen het beschrijven van het eindresultaat wederom dergelijke uitingen zal oproepen.

Eerst worden de formele op de UT geldende regels geciteerd en geanalyseerd. Dit wordt gevolgd door een overzicht van externe adviezen. Vervolgens volgt een analyse waarin de waarde van het geheimhouden van wachtwoorden wordt besproken, worden de bedreigingen in kaart gebracht en worden de voors en tegens van het frequent periodiek wijzigen van wachtwoorden belicht. Daarna volgt een overzicht van de huidige situatie op de UT, waarna een korte tekst volgt over de toekomst. Als conclusie wordt afgesloten met een aantal beleidsuitspraken.

Op een eerdere versie van dit document is feedback gegeven namens de faculteiten door Rens Brinkman, Jan Broenink en Bert Geerdink, door de informatiebeveiligingswetenschappers Pieter Hartel, Marianne Junger, Raymond Veldhuis, Wolter Pieters, Lorena Montoya, Jan-Willem Bullée en Elmer Lastdrager en door de ICTS security managers Marc Berenschot en Peter Peters. Daarnaast hebben Aiko Pras en Stefano Stramigioli aandachtspunten aangedragen.

2 Gedragscode

In de Gedragscode ICT- en Internetgebruik[4] staat het volgende over wachtwoordgebruik beschreven:

> 3.3. De door de Universiteit aan de gebruiker verleende toegangssleutel is strikt persoonlijk en blijft eigendom van de Universiteit. Het is niet toegestaan de toegangssleutel aan derden te verstrekken, tenzij dit noodzakelijk is voor een adequate uitoefening van de werkzaamheden en dan alleen na toestemming van de beheerder. Degene aan wie de toegangssleutel is verstrekt, is verplicht al hetgeen te doen dan wel na te laten wat redelijkerwijs van hem/haar mag worden verwacht om misbruik van de verstrekte toegangssleutel te voorkomen.

[3] Beleidsregels Identitymanagement Universiteit Twente, kenmerk SB/UIM/13/0213/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf
[4] Gedragscode ICT- en Internetgebruik Universiteit Twente 2009, zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_ict_mw-nl.pdf

In dit artikel wordt onder toegangssleutel de combinatie van gebruikersnaam en wachtwoord verstaan.

2.1 Strikt persoonlijk

De UT heeft ervoor gekozen de toegang tot informatie te ontsluiten via individuele gebruikersnamen met bijbehorende wachtwoorden. Dit betekent dat gebruikers deze gegevens niet aan anderen verstrekken, maar ook dat de systemen zo worden ingericht dat delegatie van taken voldoende eenvoudig mogelijk is, zodat het niet nodig is dat gebruikers hun inloggegevens aan anderen verstrekken. Dit geldt zowel voor de werkzaamheden van ICT-ondersteuners als, bijvoorbeeld, voor een onderzoeker die zekere werkzaamheden aan een secretaresse of aio wil delegeren.

2.2 Misbruik voorkomen

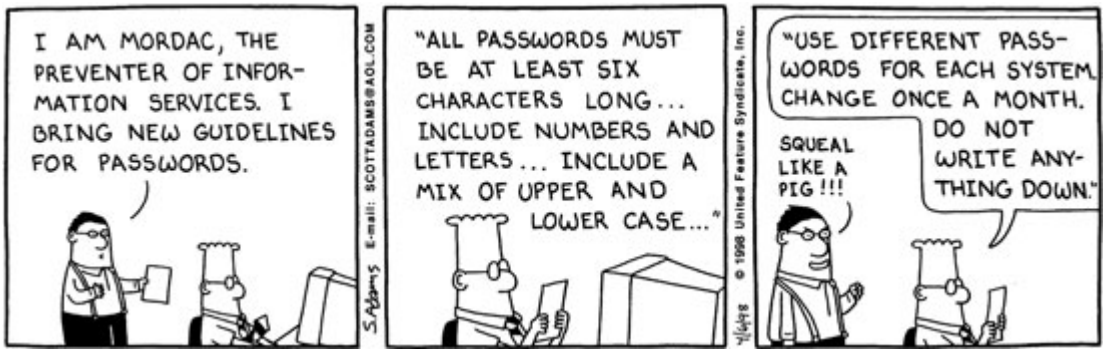
Om misbruik van wachtwoorden te voorkomen zijn vele best practices en adviezen geformuleerd. Maar wat mag redelijkerwijs van de medewerker verwacht worden? De inspanning van de medewerker zal afgewogen moeten worden tegen de belangen die op het spel staan. In de navolgende paragrafen wordt dit verder uitgewerkt.

3 Adviezen

Uit uitgelekte wachtwoorden blijkt dat de meest gebruikte wachtwoorden combinaties zijn als ‘123456’, ‘password’ en ‘qwerty’.[5] Iedereen kan begrijpen dat deze voor serieus gebruik niet goed genoeg zijn en te gemakkelijk te raden zijn. Daarom wordt doorgaans een minimale lengte en een mix van (hoofd)letters, cijfers en andere tekens afgedwongen. Veel generieke adviezen aan eindgebruikers op voorlichtingswebsites als www.digibewust.nl bepleiten dan ook complexe wachtwoorden en deze ook nog eens vaak te veranderen.

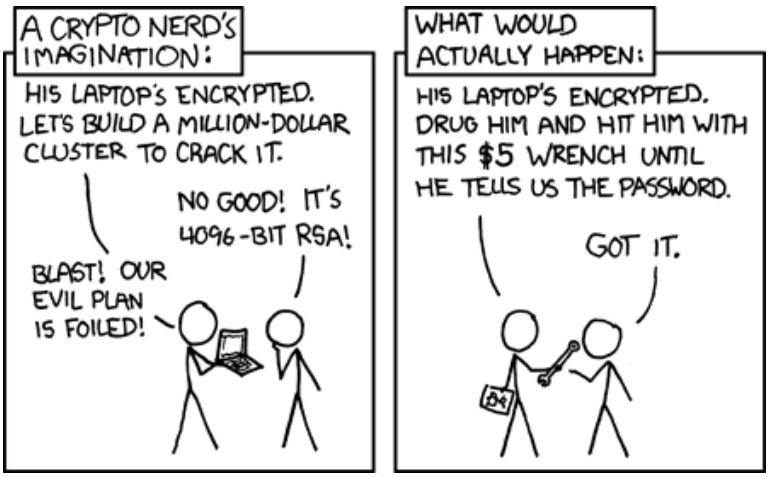
Digibewust[6] adviseert om eens in de zoveel tijd (bijvoorbeeld om de maand, of om de drie maanden) wachtwoorden te veranderen. Daarbij ook nog eens niet te voorspelbaar te worden en bijvoorbeeld geen opeenvolgende nummering te gebruiken.

Een van de Dilbert strips steekt de draak met dit soort adviezen.[7]



[5] zie http://splashdata.com/press/worstpasswords2013.htm
[6] zie http://www.digibewust.nl/index.php/onderwerpen/wachtwoorden
[7] bron: http://cryptosmith.com/archives/64

Troy Hunt stelt dat je een veilig wachtwoord niet kunt onthouden[8] en noemt de gevaren van zwakke wachtwoorden en van wachtwoordhergebruik. Daarna beschrijft hij de mogelijkheden van het gebruik van een wachtwoordkluis voor gebruikers die met veel verschillende wachtwoorden moeten werken. Vervolgens zet hij iedereen weer met beide voeten op de grond door een strip van XKCD[9] te citeren.



3.1 Accountantsadvies

KPMG, de accountant van de UT, adviseert om wachtwoorden vaak te wijzigen. Gevraagd naar de rationale kwam het volgende antwoord:

> "De norm die hieronder is opgenomen is wat mij betreft een algemene richtlijn, maar vanuit mijn persoonlijke optiek geen norm die voor alle systemen van de UT van toepassing dient te zijn. Ik vind het belangrijker dat de UT vanuit haar beleidsvorming zelf de afweging maakt welke instellingen zij willen hanteren. Voor de jaarrekeningcontrole zou ik zelf dus willen zien dat er een afweging is gemaakt waar wachtwoorden minimaal aan moeten voldoen, bijvoorbeeld geredeneerd vanuit code informatiebeveiliging.
>
> Qua good practice zie ik tegenwoordig vaak de volgende vereisten terug:
>
> - minimale lengte van 8 karakters
> - lockout na 3 keer met duration van 30m
> - wachtwoord duur van 90 tot 180 dagen
> - laatste 10 wachtwoorden mogen niet herhaald worden
> - verplicht gebruik van speciale karakters (verplicht gebruik complex wachtwoord)"

3.2 Code voor Informatiebeveiliging

ISO 27002, de Code voor Informatiebeveiliging, adviseert in §11.3.1 hoe de beheersmaatregel "Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden" verder in te vullen:

> "Alle gebruikers behoren het advies te krijgen om:
>
> a) wachtwoorden geheim te houden;
>
> b) wachtwoorden niet vast te leggen (bijvoorbeeld op papier, in bestand of in handcomputer), tenzij deze registratie veilig kan worden opgeslagen en de methode van opslag is goedgekeurd;
>
> c) wachtwoorden te wijzigen zodra er aanwijzingen zijn dat het systeem of het wachtwoord mogelijk gecompromitteerd is;

[8] The Only Secure Password Is the One You Can't Remember http://www.troyhunt.com/2011/03/only-secure-password-is-one-you-cant.html
[9] http://xkcd.com/538/

d) een wachtwoord van voldoende minimumlengte te kiezen, dat:

1) gemakkelijk te onthouden is;

2) niet is gebaseerd op iets dat iemand anders gemakkelijk zou kunnen raden of verkrijgen door gebruik te maken van persoonsgerelateerde informatie, zoals namen, telefoonnummers en geboortedata enz.;

3) niet kwetsbaar is voor woordenboekaanvallen (d.w.z. niet bestaat uit woorden die in een woordenboek voorkomen);

4) geen opeenvolgende gelijke tekens bevat en niet uitsluitend uit numerieke of alfabetische tekens bestaat;

e) wachtwoorden met regelmatige tussenpozen of op basis van het aantal malen dat men toegang tot het systeem heeft gehad te wijzigen (wachtwoorden voor accounts met speciale bevoegdheden moeten vaker worden gewijzigd dan normale wachtwoorden) en hergebruik of rouleren van oude wachtwoorden te voorkomen;

f) tijdelijke wachtwoorden bij eerste inlog te wijzigen;

g) geen wachtwoorden te gebruiken in automatische inlogprocessen, bijvoorbeeld opgeslagen in een macro of onder een functietoets;

h) geen individuele gebruikerswachtwoorden met anderen te delen;

i) niet hetzelfde wachtwoord te gebruiken voor zakelijke en particuliere doeleinden."

3.3 Discussie

De accountant noemt ook een aantal technische maatregelen, het deel wat uit de Code voor Informatiebeveiliging gekopieerd is, gaat alleen over gebruikersgedrag. Merk op dat een gebruiker adviseren iets anders is dan een gebruiker (technisch) te dwingen bepaalde beveiligingsgewoontes in acht te nemen. Gebruikers zijn slimmer dan welk algoritme dan ook en zullen, als ze daartoe voldoende gemotiveerd zijn, manieren vinden om regels te omzeilen of krachteloos te maken. In een onderzoek van Microsoft Research wordt beschreven dat dit uit het oogpunt van de gebruiker op grond van economische motieven in zijn algemeenheid rationeel is.[10] Bij een advies hoort dus altijd een rationale, waarom is een bepaald gedrag gewenst. Veel adviezen worden gegeven zonder aan te geven waarom deze relevant zijn, vanuit een soort militair need-to-know principe. Uit onderzoek van het University College of London blijkt dat gebruikers dergelijke adviezen niet opvolgen.[11]

4 Analyse

4.1 Waarde

Wat is de waarde van wachtwoorden? Wat is de waarde van de UT-gebruikersnaam met bijbehorende wachtwoord? E-mail wachtwoorden worden voor $4–$30 op de zwarte markt verkocht.[12] De kosten voor een organisatie die op een zwarte lijst geplaatst wordt en daardoor (tijdelijk) niet kan e-mailen zijn natuurlijk vele malen hoger.

Bij het bepalen van de waarde gaat het er natuurlijk niet om hoeveel het de crimineel kan opleveren, maar hoeveel schade de gebruiker en de UT kunnen lopen als een account gecompromitteerd wordt.

Buiten de publicitaire schade, kan dan gedacht worden aan de volgende risico's:

[10] So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. Cormac Herley. Proceedings New Security Paradigms Workshop, 2009, pp.133-144. zie http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf

[11] Users are not the enemy. Adams, A; Sasse, MA. Communications Of The ACM, 1999, Vol.42(12), pp.41-46

[12] zie http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf

- je wilt niet dat je emailaccount wordt misbruikt door spammers;
- je wilt niet dat studenten hun tentamenresultaten kunnen aanpassen;
- je wilt niet dat je bankrekeningnummer waar je salaris op gestort wordt door iemand anders wordt aangepast;
- je wilt niet dat studenten van te voren de vragen van een tentamen kunnen inzien;
- als je toegang hebt tot vertrouwelijke (persoons)gegevens in Osiris, Oracle Applications of Decos dan wil je voorkomen dat deze openbaar worden;
- je wilt niet dat je onderzoeksdata (voortijdig) openbaar worden en al helemaal niet dat deze door onbevoegden aangepast worden.

Dit soort argumenten zal in de voorlichting aan gebruikers gebruikt moeten worden om het belang van het vertrouwelijk houden van wachtwoorden te illustreren.

4.2 Bedreigingen

Als we accepteren dat de waarde van het UT-wachtwoord groot genoeg is om moeite voor te doen om te beschermen, zijn de eerder genoemde adviezen dan zinnig of zijn het security mythes die slechts op folklore en bijgeloof berusten, zoals Gene Spafford[13] beweert? Voordat adviezen op waarde geschat kunnen worden, zal helder moeten zijn op welke manier een wachtwoord gecompromitteerd kan worden. Effectieve beveiliging betekent dat tegen alle mogelijke bedreigingen tegen de vertrouwelijkheid van wachtwoorden maatregelen worden genomen.

Het NIST heeft deze bedreigingen gedetailleerd in kaart gebracht[14] en onderscheidt het *buitmaken* van wachtwoorden, het *raden en kraken* en het *vervangen* van wachtwoorden.

Een wachtwoord opgeslagen in de browser of onversleuteld tekstbestand kan worden buitgemaakt wanneer toegang wordt verkregen tot de PC, bijvoorbeeld middels een virus of als het apparaat wordt gestolen. Tijdens het invoeren kan een wachtwoord worden buitgemaakt door een keylogger die iedere toetsaanslag registreert of door schoudersurfen, bijvoorbeeld als iemand in de trein met je meekijkt op je tablet of mobieltje. Daarnaast kunnen wachtwoorden worden buitgemaakt door social engineering, bijvoorbeeld door een phishingmail te versturen en gebruikers te verleiden hun gegevens op een website in te voeren.

Met raden wordt bedoeld het herhaaldelijk opnieuw proberen of een wachtwoord juist is. Hier wordt doorgaans tegen beveiligd door het aantal pogingen te beperken. Met kraken wordt bedoeld het met brute kracht uitproberen van een buitgemaakt wachtwoordbestand. Hier wordt doorgaans tegen beveiligd door hashing toe te passen (en geen omkeerbare versleuteling van wachtwoorden). Het gebruik van salting tijdens het hashproces maakt het kraken nog moeilijker. Adviezen die gegeven worden over wachtwoordsterkte werken alleen tegen raden en kraken.

Vervangen kan bijvoorbeeld door een malafide helpdeskmedewerker of, als de organisatie de procedure om vergeten wachtwoorden te resetten niet goed op orde heeft, de helpdesk te social engineeren.

Op de UT zijn er een flink aantal medewerkers die hun wachtwoord op een geeltje noteren en dit in de buurt van het beeldscherm of in een la bewaren. Collega's hebben er dan toegang toe en procedures omtrent functiescheiding kunnen dan makkelijk doorbroken worden. Daarnaast delen meerdere leidinggevenden hun wachtwoord met een secretaresse omdat systemen niet allemaal ingericht zijn op de mogelijkheid van delegatie van verantwoordelijkheden.

In de Beleidsregels Identitymanagement zijn al veel technische maatregelen beschreven. Doordat de UT zoveel mogelijk Single Sign On (SSO) gebruikt en de wachtwoorden voor de overige systemen zoveel mogelijk synchroniseert, hoeven de meeste gebruikers voor de UT maar één complex wachtwoord te onthouden. Het nadeel van SSO is dat het wachtwoord nog waardevoller wordt: als er iets fout gaat dan gaat het goed fout.

[13] Security Myths and Passwords, zie http://www.cerias.purdue.edu/site/blog/post/password-change-myths/ en Passwords and Myth, zie http://www.cerias.purdue.edu/site/blog/post/passwords-and-myth/
[14] SP 800-118 DRAFT Guide to Enterprise Password Management, zie http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

De risico's van phishing en het gebruik van geeltjes zijn alleen te ondervangen door voorlichting aan gebruikers.

4.3 Periodiek wijzigen van wachtwoorden

Zoals het NIST beschrijft is het regelmatig moeten wijzigen van wachtwoorden een bron van frustratie voor gebruikers. Het vergt een actieve afweging van de risico's en de gebruikersvriendelijkheid of het periodiek wijzigen van wachtwoorden verplicht wordt gesteld en zo ja welke periode er gekozen wordt. Zoals Gartner[15] opmerkt is het verplicht wijzigen het meest controversiële aspect van wachtwoordbeleid. Dit is ook op de UT het geval en is dan ook de reden dat de Beleidsregels Identitymanagement van eind 2013 voor wat betreft de periodiciteit van het wijzigen van wachtwoorden slechts de staande praktijk beschrijven.

Het idee van een wachtwoord vaak veranderen is dat als een bestand met versleutelde wachtwoorden wordt buitgemaakt dat dan de wachtwoorden gevonden moeten worden voordat deze weer gewijzigd zijn. In de praktijk kunnen echter binnen enkele uren de meeste wachtwoorden gevonden worden.[16] Een ander argument is dat als het wachtwoord van een gebruiker uitlekt dat het dan maar gedurende een beperkte tijd misbruikt kan worden. In veel gevallen wordt het misbruik onmiddellijk gepleegd, dan helpt het vaak veranderen niet. Bovendien zorgt vaak veranderen voor problemen met het onthouden en leidt het er vaak toe dat gebruikers volgnummers gaan gebruiken en/of het wachtwoord gaan opschrijven.

Gartner beschrijft dat als een organisatie kiest voor geen of een lage wijzigingsfrequentie, dat dan wel de overige processen robuust moeten zijn ingericht en dat alle voorzorgsmaatregelen zijn genomen. Zelfs in dat geval beveelt Gartner een infrequente, zeg jaarlijkse, verplichte wijziging aan als laatste veiligheidsnet. Het IDM systeem is nu ingericht overeenkomstig dit Gartner advies.

5 Huidige UT-praktijk

Volgens het beleid[17] hebben UT-gebruikers één gebruikersnaam en wordt zoveel mogelijk Single Sign-On toegepast. ICTS werkt nog aan de implementatie van dit vastgestelde beleid. Daarmee hoeven gebruikers voor UT-systemen maar één wachtwoord te onthouden. Wachtwoorden worden altijd via een beveiligde verbinding verstuurd.

Eén keer per jaar verloopt het UT-wachtwoord. Vanaf een maand van te voren ontvangen gebruikers aankondigingen dat het wachtwoord vernieuwd moet worden.[18] De noodzaak van vernieuwen komt dan ook niet als een verrassing, gebruikers hebben de tijd om over een nieuw wachtwoord na te denken.

5.1 Complexiteit

De UT hanteert[19] de volgende regels ten aanzien van de complexiteit van wachtwoorden:

- Een wachtwoord moet uit minimaal 8 karakters en maximaal 16 karakters. bestaan
- Het nieuwe wachtwoord moet anders zijn dan uw voorgaande 3 wachtwoorden van uw domeinaccount en verder voldoen aan drie van de volgende vier eisen:
  - 1 of meer speciale karakters (!,$,#,%)
  - 1 of meer cijfers (0-9)
  - 1 of meer hoofdletters (A-Z)
  - 1 of meer kleine letters (a-z)

[15] Best Practices for Managing Passwords: Policies Must Balance Risk, Compliance and Usability Needs. G00201000, Gartner, 15 juli 2010.
[16] zie http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/
[17] zie Beleidsregels Identitymanagement Universiteit Twente http://www.utwente.nl/uim/informatiebeveiliging/Beleidsregels-Identitymanagement-Universiteit-Twente.pdf
[18] zie Verlopen wachtwoord http://www.utwente.nl/icts/servicedesk/idm/
[19] zie http://www.utwente.nl/icts/itsecurity/actueel/beleid/policies/Samenstel wachtwoorden 2012 04 02-1/

Tegen deze complexiteitseisen bestaat geen weerstand, al wensen sommigen een langer wachtwoord, maar dat is technisch helaas niet haalbaar.

5.2 Externe accounts

Voor het gebruik van systemen buiten de UT moet vaak nog een apart account aangemaakt worden. De UT streeft door integratie met SURFconext ernaar dat gebruikers met hun UT-account kunnen inloggen. Voor een groot deel van de externe webapplicaties bestaat deze mogelijkheid niet. Medewerkers en studenten moeten tientallen tot honderden gebruikersnamen, wachtwoorden en pincodes onthouden. De cognitieve belasting daarvan is significant. De UT wil deze belasting zo laag mogelijk houden.

Door het gebruik van een wachtwoordkluis te stimuleren kunnen gebruikers ondersteund worden bij het veilig opslaan van wachtwoorden. ICTS kan voorlichting geven op de website en de benodigde software aanbieden ter installatie. Een alternatief voor een wachtwoordkluis is het opschrijven van wachtwoorden op papier. Dat kan immers niet gehackt worden en is voor iedereen te begrijpen. Daarom wordt opschrijven op papier door beveiligingsgoeroes als Bruce Schneier[20] en anderen[21] geadviseerd.

5.3 Gebruikers

Het wijzigen van het wachtwoord kost medewerkers, zeker als het op meerdere apparaten voor VPN, wifi en mail is ingesteld, jaarlijks een significante hoeveelheid tijd. Sommigen hebben hierbij ondersteuning van de ICTS-servicedesk nodig. Hoewel het verplichte jaarlijkse wijzigen van wachtwoorden eigenlijk geen echte beveiligingsvoordelen biedt, wil de UT deze verplichting niet laten vervallen. Het is immers een veelgegeven advies en een bestaande geïmplementeerde maatregel.

Het voordeel dat alle UT-systemen hetzelfde wachtwoord gebruiken is dat dit wachtwoord vaak ingetikt moet worden, daardoor gaat het onthouden vanzelf. Gebruikers geven nog regelmatig hun wachtwoord af aan collega's, omdat nog niet alle systemen er op ingericht zijn dat delegatie van werkzaamheden mogelijk is. Dit brengt grote risico's met zich mee. Het belang om de systemen zo in te richten dat delegatie van werkzaamheden wel mogelijk is, is beschreven in de Beleidsregels Identitymanagement Universiteit Twente. Er wordt te weinig voorlichting aan gebruikers gegeven over het belang van het geheimhouden van wachtwoorden. De risico's en diverse scenario's van social engineering moeten hierbij ook belicht worden. Er hoort op de UT geen scenario te bestaan waarbij het aanvaardbaar is iemand anders om zijn of haar wachtwoord te vragen.

Gebruikers willen een duidelijk advies hoe met hun wachtwoorden om te gaan. ICTS zal een wachtwoordkluis moeten adviseren en aanbieden. De risico's van het opslaan van wachtwoorden op papier bij monitor of toetsenbord, in een onbeveiligd tekstbestandje of in de browser zullen hierbij ook aan de orde moeten komen.

6 Toekomstige ontwikkelingen

In de zorg wordt de UZI-pas gebruikt waarmee zorgverleners zich digitaal kunnen identificeren. Bij de UT wordt een digitaal pasje voor identificatie nog alleen bij het printen gebruikt en niet voor toegang tot informatiesystemen. Internationaal ontwikkelt de FIDO (Fast IDentity Online) Alliance[22] standaarden om de afhankelijkheid van wachtwoorden te verminderen. Er wordt door partijen als Microsoft en Google naar gestreefd[23] om het gebruik van wachtwoorden grotendeels overbodig te maken. Bij de printers identificeert men zich al alleen met een eigen gekozen pasje, voor het gekozen doel is dat goed genoeg.

[20] zie https://www.schneier.com/blog/archives/2005/06/write_down_your.html
[21] zie http://www.vox.com/2014/4/16/5614258/the-best-defense-against-hackers-writer-your-passwords-down-on-paper
[22] zie https://fidoalliance.org/about
[23] zie http://www.theverge.com/2014/4/15/5613704/the-plot-to-kill-the-password

In Nederland ontwikkelt SURFnet multifactor authenticatie voor cloudapplicaties via SURFconext.[24] Er lopen inmiddels enkele pilotprojecten. Als tweede factor kan bijvoorbeeld een token gelden wat afhankelijk van het moment een code afgeeft. Een andere mogelijkheid is het gebruik van SMS.

Om te voorkomen dat de UT voor allerlei verschillende systemen verschillende technieken gaat gebruiken, kiest de UT ervoor om aan te sluiten bij de SURFnet ontwikkelingen en geen leverancierspecifieke beveiligingstechnieken te gebruiken.

Voor sommige toepassingen is maar heel weinig authenticatie nodig. Dan kan een cookie met een relatief lange geldigheidsduur voldoende zijn. Voor andere toepassingen is juist veel zekerheid omtrent de identiteit nodig, voor de afgifte van een token kan bijvoorbeeld geëist worden dat deze persoonlijk afgehaald moet worden. In de Handreiking betrouwbaarheids-niveaus[25] worden use-cases uit het Hoger Onderwijs- en Onderzoek (gebaseerd op de referentiearchitectuur HORA) besproken.

7 Conclusie

1. Op termijn zal de UT gebruik maken van multifactorauthenticatie op basis van vastgestelde betrouwbaarheidsniveaus. De UT volgt hierbij de ontwikkelingen bij SURFnet.
2. Voorlopig zal de UT voor de authenticatie van gebruikers wachtwoorden blijven gebruiken.
3. De verplichting aan gebruikers om het wachtwoord eens per jaar te wijzigen vervalt niet.
4. De complexiteit van wachtwoorden die de UT afdwingt is voldoende en hoeft niet aangepast te worden.
5. Wanneer er aanwijzingen zijn dat hun wachtwoord is gecompromitteerd dan dienen gebruikers het dwingende advies te krijgen dit te wijzigen.
6. Voorlichting over de waarde van wachtwoorden, de noodzaak deze vertrouwelijk te houden en het UT-wachtwoord niet elders te gebruiken moet bij de UT worden geïntensiveerd.
7. Voorlichting over de mogelijkheden van een wachtwoordkluis en het aanbieden van de betreffende software moet bij de UT worden geïntensiveerd.
8. De uitspraken in de Beleidsregels Identitymanagement Universiteit Twente over wachtwoorden worden voor zo ver relevant aangepast.

[24] Presentatie Eefje van der Harst, Beveiligingsconferentie SURFcert & SURFibo, februari 2014, zie http://www.surf.nl/binaries/content/assets/surf/nl/2014/presentatie-surfcert-surfibo-2014-multi-factor-authenticatie-voor-cloudapplicaties-via-surfconext---eefje-van-der-harst.pdf

[25] zie http://www.surf.nl/nieuws/2014/02/hoe-veilig-moet-de-toegang-tot-een-online-dienst-zijn.html