TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Westfriesgasthuis
Jaarverslag 2016

Veilige informatievoorziening bij Westfriesgasthuis

Het Westfriesgasthuis te Hoorn is een algemeen ziekenhuis met een opnamecapaciteit van 506 erkende bedden en ongeveer 258.000 polikliniekbezoeken per jaar. Om de doelstelling één van de veiligste ziekenhuizen te worden te behalen, startte het Westfriesgasthuis enkele jaren terug een grootschalig veiligheidsproject, waarbij zowel authenticatie als User Account Provisioning geprofessionaliseerd werden. Rob Kuijpers, senior unithoofd Informatisering vertelt: "Destijds bestonden er veel algemene afdelingsaccounts. Dat speelde voornamelijk op de verpleegafdelingen, omdat het daar niet werkbaar is om steeds in- en uit te loggen. Wij wilden af van deze onveilige situatie." Naast het afschaffen van algemene afdelingsaccounts wilde het Westfriesgasthuis wijzigingen die consequenties hebben op fysieke en digitale toegangsrechten beter vastleggen. "Met name als medewerkers van functies wijzigden of als zij ons ziekenhuis verlieten, werd er geen actie ondernomen om de logische en fysieke toegang te wijzigingen of te ontnemen," aldus Rob Kuijpers. "Dat kwam omdat de berichtgeving vanuit P&O hierover foutgevoelig was." Het laatste probleem was dat bij het toekennen van rechten vaak de rechten overgenomen werden van medewerkers in soortgelijke functies.

Authenticatie en autorisatie

Rob Kuijpers: "De eerste stap naar de gewenste situatie was het elimineren van de algemene accounts door alle gebruikers een toegangspas te geven die vereist is voor fysieke en digitale toegang. Gebruikers krijgen alleen een toegangspas wanneer zijn hun identiteitsbewijs voorleggen. Gelijktijdig met de pas werd ook een nieuwe Citrix-omgeving ingevoerd, die gebruikers in staat stelt hun openstaande sessie 'mee te nemen' naar een andere pc.

Klant
Westfriesgasthuis

Uitdaging
De werkmethodes die werden gebruikt (algemene accounts, kopiëren van rechten) voldeden niet aan de eisen van het nieuwe veiligheidsbeleid.

Oplossing
Accounts en toegangsrechten van medewerkers automatisch aanmaken op basis van de gegevens in het personeelssysteem zoals functie, afdeling/ kostenplaats en rol.

Product
UMRA
- Auto Provisioning (SRC)
- Downstream Provisioning (APPL)
- Role Based Access Control (RBAC)
- Workflow Management (WFM)

Koppelingen
Active Directory
iProtect
Ultimo
EduManager
CS-EZIS

Resultaat
Voldoen aan nieuw veiligheidsbeleid voor digitale en fysieke toegang, kunnen werken volgens een bepaalde standaardisatie werken en betere serviceverlening naar de organisatie.

“In de eerste fase werd een koppeling gemaakt tussen ons personeelssysteem Beaufort, de Active Directory en Iprotect. Momenteel zijn we bezig om RBAC in te richten.”

Rob Kuijpers
Senior Unithoofd Informatisering bij Westfriesgasthuis

Rob Kuijpers: “De eerste stap naar de gewenste situatie was het elimineren van de algemene accounts door alle gebruikers een toegangspas te geven die vereist is voor fysieke en digitale toegang. Gebruikers krijgen alleen een toegangspas wanneer zijn hun identiteitsbewijs voorleggen. Gelijktijdig met de pas werd ook een nieuwe Citrix-omgeving ingevoerd, die gebruikers in staat stelt hun openstaande sessie ‘mee te nemen’ naar een andere pc.

De tweede stap was een User Account Provisioning project met als uitgangspunt dat de accounts en toegangsrechten van medewerkers (in zowel Active Directory, het zorginformatiesysteem CS-EZIS, helpdeskpakket Ultimo, security management systeem iProtect als e-learningsysteem EduManager) automatisch aangemaakt worden op basis van de gegevens in het personeelssysteem zoals functie, afdeling en kostenplaats. De daaraan gekoppelde rechten in de autorisatiematrix, afgesproken standaarden en conventies vormen de basis voor het automatisch aanmaken van een e-mailadres en account met alle bijbehorende autorisaties. Deze kunnen vervolgens worden aangevuld en gecontroleerd via een workflow door bijvoorbeeld de manager.

Het ziekenhuis schreef hier een RFP voor uit en uiteindelijk viel de keus op UMRA door de kleinere behapbare fases die Tools4ever hanteert. Rob Kuijpers: “In de eerste fase werd een koppeling gemaakt tussen ons personeelssysteem Beaufort, de Active Directory en iProtect.” Wanneer P&O een medewerker toevoegt, gegevens wijzigt of verwijdert in Beaufort, neemt UMRA de juiste actie in het netwerk. Tevens worden signalen uit het HR-systeem omgezet in directe acties naar de beheerder van iProtect, zodat deze een nieuwe medewerker kan registreren. “Hiernaast ontvangt de IT-afdeling nu nog een papieren goedkeuring van de accountaanvraag van een manager, waarna de helpdesk nog de benodigde applicaties aan het profiel hangt”, aldus Rob Kuijpers. “Deze laatste stap is nu nog handmatig, maar wij zijn op dit moment samen met Tools4ever aan het analyseren welke pakketten en welke rechten iemand heeft binnen het ziekenhuis, binnen een afdeling, binnen een functie en binnen een rol om Role Based Access Control (RBAC) in te kunnen richten. Als we dat in kaart hebben gebracht, kunnen bepaalde applicaties en systemen of toegang tot fysieke locaties al standaard worden toegevoegd aan een account.”

Workflow Management en Role Based Access Control

In het vervolgtraject wordt het Workflow Management gedeelte van UMRA geïmplementeerd. Dat betekent dat de papieren goedkeuringsbriefjes komen te vervallen. Op basis van informatie uit het HR-systeem krijgt een manager bij in-diensttreding van een nieuwe medewerker een notificatie e-mail met een link naar het autorisatiedashboard. In het autorisatiedashboard zijn de rechten die gelden voor de nieuwe medewerker op basis van zijn rol reeds ingevuld. De manager kan indien nodig extra rechten toevoegen. Na het aanvinken van de benodigde rechten start een workflow en dienen de betrokken resource eigenaren (bijvoorbeeld share owner of licentiebeheerder) voor specifieke rechten goedkeuring te verlenen. Hierna worden de rechten automatisch toegekend en wordt het gehele aanvraagproces met alle goedkeuringen gelogd voor audit doeleinden.

Tools4ever BV
Amalialaan 126C
3743 KJ Baarn
Nederland

Website: tools4ever.com
Informatie: info@tools4ever.com
Sales: sales@tools4ever.com
Tel: +31 (0) 35 54 832 55