Whitepaper

Hoe processen en efficiency te verbeteren in de zorg.

Uit onderzoek naar de toepasbaarheid van identity en access management en aanverwante authenticatie technologie bij diverse zorginstellingen in Nederland zijn Authasas en ngage tot een aantal opzienbarende conclusies gekomen.

Allereerst blijkt de automatiseringsgraad in de zorg en de juiste gebruikmaking van aanwezige informatie(systemen) en technologieën er over het algemeen slecht voor staan. Hoewel er met de recente wijzigingen in wet- en regelgeving erg veel eisen gesteld worden aan privacy en certificering ligt de nadruk nog vaak op het behalen van het certificaat en te weinig op de daadwerkelijke verbetering van processen en controleerbaarheid.

Voorts kan het bewustzijn en de vooruitziende blik in deze sector ten aanzien van integratie in het algemeen en identity en access management in het bijzonder nog aanzienlijk verbeterd worden. Waar in andere sectoren de bedoelde technologie zich al ruimschoots bewezen heeft, blijkt men in de zorg nog erg in hokjes en point-solutions te denken en de verantwoordelijkheid voor toegang en beveiliging vooral niet te willen delen met ervaren automatiseringspartners. Dat is althans de algemene teneur onder leveranciers van op de zorg gerichte informatiesystemen (o.a. EPD, ECD, EVS, etc.).

De klanten

In de praktijk houdt dit bijvoorbeeld in dat afdelingen dagelijks bezig zijn met het beheer van medewerkers en de gebruikersaccounts in de diverse informatiesystemen. Deze worden handmatig onderhouden evenals de toekenning van de vereiste rollen en rechten. Daarnaast is ICT beheer verantwoordelijk voor het aanmaken van mailboxen, gebruikersaccount, directories, home directories en het toekennen van rechten en rollen.

Dit proces vindt dan bij verandering of het beëindigen van de functie wederom handmatig en zelfs in omgekeerde volgorde plaats met het gevolg dat de rechten veelal niet tijdig worden toegekend of ontnomen.

Het beeld dat in de instellingen bij deze werkwijze in stand wordt gehouden is vaak gericht op de legitimering hiervan. Het is tenslotte de ultieme manier om de controle te houden, althans zo houdt men vol. Vertrouwen in bewezen identity management oplossingen met provisioning en deprovisioning, role based access en identity lifecycle management ontbreekt vaak.

Belangrijke complicatie van het ontbreken van een grote mate van automatisering is dat authenticatie-oplossingen in combinatie met single sign on hier van afhankelijk zijn. Met overal losse systemen en accounts is authenticatie niet goed te regelen.

Trajecten m.b.t. authenticatie-oplossingen stranden vaak op het feit dat aan dergelijke voorwaarden (nog) niet voldaan wordt.

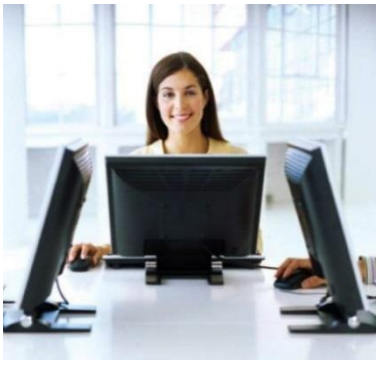
Deze organisaties wijken dan vaak uit naar oplossingen die alleen het gebruiksgemak vergroten, maar de processen en beveiliging niet verbeteren. Dit zijn op zichzelf staande single sign on oplossingen, wachtwoordmanagers of een enkele koppelingen die zich nog het best als maatwerk laten omschrijven met alle gevolgen voor het toekomstig onderhoud van dien.

De leveranciers

Uit deze onderzoeken blijkt dat de grote leveranciers van informatiesystemen – vaak niet uitsluitend op de zorg gericht, maar op diverse sectoren – hedendaagse technologie ondersteunen. Denk hierbij aan de makkelijk toegankelijke Active Directory Federation Services van Microsoft, SAML, XML en SOAP koppelingen, etc.

De wat kleinere partijen – waaronder ook verticale oplossingen van grotere merken – hanteren gewoonlijk een batchgewijze uitwisseling van bestanden met gegevens, waarbij de batch op commando op ieder gewenst moment kan worden uitgevoerd.

Hierbij is gewoonlijk sprake van eenrichtingsverkeer.



Het is de norm om binnen de applicaties een eigen vorm van gebruikersbeheer aan te bieden en hiermee kan vaak niet goed door externe toepassingen worden gecommuniceerd. Het aanmaken van gebruikers in de applicaties en het toekennen van rollen en rechten beschouwen de meeste leveranciers als een verantwoordelijkheid van de eigen applicatie, waardoor dit handmatig door een manager uitgevoerd moet worden.

De visie

Zoals door Authasas en ngage al bij vele organisaties is aangetoond bestaan er zeer veilige oplossingen om informatiesystemen te koppelen met het centrale automatiseringssysteem. Hierbij wordt gebruikersbeheer aangedreven vanuit een centraal systeem – gewoonlijk het HRM product – en wordt op basis van functies een vertaling naar rollen en rechten in de diverse systemen gemaakt. Dit gebeurt met standaard producten die sinds eind vorige eeuw in ontwikkeling zijn, waardoor de oplossing goed te onderhouden is en eenvoudig uitbreidbaar.

Wij nodigen zorgverlenend Nederland van harte uit voor een gesprek over de mogelijkheden om een daadwerkelijke en structurele verbetering te realiseren op het gebied van beveiliging, gebruikersbeheer en toegang tot informatiesystemen. Niet alleen bespaart u kosten en verhoogt u de kwaliteit en veiligheid van uw informatievoorziening, maar bovendien is uw client het waard!

Voor meer informatie:

www.authasas.com
info@authasas.com

www.ngage.nl
info@ngage.nl