

'Single sign-on' is een alternatief voor het onthouden van veel complexe wachtwoorden. Veiliger is het ook. Hoewel veel IT-managers en security officers daaraan twifelen. Ten onrechte, zegt **Arnout van der Vorst**. Er bestaan nogal wat vooroordelen met betrekking tot een 'single sign-on'-implementatie. Van der Vorst bespreekt er zes.

Zes vooroordelen over 'single sign-on'

SSO kan zeer eenvoudig en kleinschalig aan het begin van een proces worden ingezet

Bij 'single sign-on' (SSO) loggen eindgebruikers eenmaal in met hun credentials waarna zij direct toegang hebben tot al hun applicaties en systemen zonder dat gevraagd wordt om opnieuw in te loggen. Het is een mooie oplossing voor de vele wachtwoorden die eindgebruikers tegenwoordig moeten onthouden. Echter, dat is voor organisaties geen reden om klakkeloos een SSO-oplossing te implementeren. Veel IT-managers en security officers zijn namelijk sceptisch over de implementatie van een 'single sign-on'-oplossing. De sceptische houding is het gevolg van een aantal vooroordelen dat over SSO de ronde doet. In veel gevallen zijn deze vooroordelen onjuist. Veelgehoorde vooroordelen van IT-managers bij grote en middelgrote bedrijven zijn de volgende:

1 Het toepassen van SSO legt een grotere druk op security

IT-managers en vooral security officers denken dat met het openstellen van het applicatielandschap met een eenmalige login ook direct de beveiliging van informatie in gevaar is. Want wanneer een ongeautoriseerd persoon de enig overgebleven logingegevens in handen krijgt, heeft hij toegang tot alle gekoppelde applicaties. Vooral het feit dat hiermee bedrijfskritische informatie openstaat, leidt tot weerstand. Bij SSO worden alle verschillende toegangspunten tot applicaties vervangen door één toegangspunt. Dit lijkt inderdaad een risico, maar de kans dat eindgebruikers de enkele logingegevens die zij nodig hebben voor SSO, op een briefje onder hun toetsenbord bewaren, is veel kleiner dan de circa twaalf wachtwoord- en usernamecombinaties die zij nodig hebben zonder SSO. Om de kritische applicaties en applicaties met privacygevoelige informatie te beschermen, is het mogelijk om de primaire SSO-login extra te beveiligen met een gebruikerspas en pincode of een extra sterk (complex) wachtwoord. Het inloggen middels een pas en pincode is een erg sterke authenticatie en wordt daarnaast door gebruikers als zeer gebruiksvriendelijk ervaren.

2 Een SSO-implementatie is een langdurig project

Een SSO-implementatie is vaak een onderdeel van een breder securitybeleid. Andere onderdelen kunnen zijn: het invoeren van complexere wachtwoorden, netter omgaan met autorisaties en het voldoen aan normen die door de overheid zijn opgelegd. Omdat SSO bijna alle eindgebruikers raakt en dwars door de organisatie heen

loopt, vergt het veel tijd om die eindgebruikers te informeren en voor te bereiden. Tevens brengt SSO veel vragen met zich mee, zoals 'Hoe moet ik omgaan met mensen die meerdere logins hebben op één applicatie?', 'Wat doe ik als een applicatie die middels SSO wordt aangeboden een nieuwe versie krijgt?' en 'Wat gebeurt er als binnen de applicatie wordt gevraagd om het resetten van het wachtwoord?' Dit zorgt ervoor dat een SSO-implementatie vaak naar de achtergrond verschuift. De mogelijke complexiteit van het project is echter geen reden om de implementatie ervan uit te stellen. Door klein te beginnen – zeg de topijfapplicaties beschikbaar maken middels SSO – is al een aanzienlijke tijdsbesparing van het aantal loginmomenten, waarmee de aanschaf van de oplossing is te rechtvaardigen.

Stringenter wachtwoordbeleid resulteert direct tot meer calls naar de helpdesk

3 Het is niet mogelijk cloud-applicaties via SSO beschikbaar te maken

Het is begrijpelijk dat men dit denkt, want er bestaan tegenstrijdige verhalen over. Er is een groep experts die meent dat cloudapplicaties 'federated' aangeboden moeten worden en een groep die zegt dat cloudapplicaties via connectors toegankelijk gemaakt kunnen worden. Uit de tegenstrijdige berichten blijkt dat de impact van 'de cloud' in combinatie met SSO nog onduidelijk is. Maar één ding is wel duidelijk: de SSO-login naar cloudapplicaties is net als bij iedere andere applicatie mogelijk.

4 Een SSO-implementatie is duur

Het mooie aan een SSO-oplossing is dat het vaak niet nodig is om die voor alle mensen in de organisatie in te richten. In een ziekenhuis bijvoorbeeld is SSO slechts voor een selecte groep noodzakelijk. Het advies is: beperk je tot de meest kritische applicaties en tot die mensen die op veel verschillende applicaties moeten inloggen. Dan is de implementatie in prijs en complexiteit goed

te overzien. Vervolgens biedt dit een prima startpunt voor eventuele groei en uitbreiding in overeenstemming met wijzigende behoeften in de toekomst.

5 Het is beter de ontwikkelingen rond SSO af te wachten

Veel organisaties nemen een afwachtende houding aan als het gaat om SSO. Zij kijken wat andere bedrijven in hun sector doen. Ziekenhuizen bijvoorbeeld wachten op de ontwikkelingen ten aanzien van de persoonlijke UZI-pas (het elektronisch authenticatiemiddel voor de zorg) die door de overheid wordt geïntroduceerd. De introductie van de persoonlijke UZI-pas binnen het ziekenhuis kan een mooie aanleiding zijn om voor eindgebruikers applicaties via SSO (met pas) beschikbaar te maken. Andere bedrijven wachten misschien eerst totdat de implementatie van een andere kritisch systeem (bijvoorbeeld ERP of HR) is afgerond. SSO is dan een laatste stap in het proces. SSO kan echter al zeer eenvoudig en kleinschalig aan het begin van het proces worden ingezet. Vervolgens is het mogelijk om alle applicaties die nieuw worden geïmplementeerd via SSO beschikbaar te maken, zonder daarvoor grote aanpassingen te hoeven doen.

6 Een SSO-oplossing is niet nodig want wij gebruiken extreem complexe wachtwoorden

Het eisen van extreem complexe wachtwoorden is een van de mogelijkheden om het netwerk te beveiligen, maar is daarbij ook een van de oorzaken van onveilige situaties. Veel eindgebruikers hebben moeite met het onthouden van deze wachtwoorden, zeker wanneer zij meer dan acht wachtwoord- en usernamecombinaties dienen te onthouden. Vaak resulteert een stringenter wachtwoordbeleid direct tot meer calls naar de helpdesk, omdat mensen hun wachtwoord vergeten. Een zeer onveilige en ongewenste situatie ontstaat wanneer eindgebruikers de wachtwoorden noteren op Post-its en rond hun computer laten slingeren. In dit soort gevallen biedt SSO een eenvoudige oplossing.

Arnout van der Vorst (a.vandervorst@tools4ever.com) is technical consultant bij Tools4Ever, expert op het gebied van Identity & Access Management.



Fast User Switching

Specialisten in de zorg hebben snel toegang nodig

Normeringen die worden opgelegd vanuit de overheid (bijvoorbeeld NEN 7510 binnen de zorg) eisen dat ieder individu die toegang heeft tot gevoelige (patiënten)informatie, geïdentificeerd moet kunnen worden en dat de details van de toegang (wanneer, welke actie) worden gelogd. Groepsaccounts mogen daardoor niet langer worden ingezet. In ziekenhuizen komt het gebruik van generieke accounts veelvuldig voor. Zo maakt al het personeel op een eerste hulp gebruik van één pc en omwille van de snelheid wordt niet steeds aan- en uitgelogd. In een normale kantooromgeving zijn de opstarttijden vervelend maar acceptabel. In afwijkende omgevingen zoals in de operationele industrie of in de zorg waar een pc gedeeld wordt door meerdere medewerkers, is dit niet acceptabel. Specialisten hebben uit het oogpunt van patiëntenzorg snel (binnen acht seconden) toegang nodig tot de patiënteninformatie. In dit geval biedt een functionaliteit van single sign-on, genaamd Fast User Switching, een uitkomst.

Deze functie biedt gebruikers de mogelijkheid om snel aan- en af te loggen van openbare computers. Wanneer gebruikers aanloggen met behulp van Fast User Switching, worden applicaties die zij nodig hebben direct en automatisch opgestart en aangemeld. Wanneer gebruikers uitloggen, kan de SSO-oplossing uitloggen van de applicaties en/of de applicaties sluiten. Een vereenvoudiging van de inlogprocedures kan verkregen worden met Fast User Switching in combinatie met een willekeurige gebruikerspas (bijvoorbeeld de UZI-pas), waarmee de gebruiker door middel van het invoeren van de gebruikerspas toegang krijgt tot de gewenste applicaties. Het verwijderen van de pas betekent uitloggen en de computer beschikbaar stellen aan een andere medewerker. De 'Follow Me'-functionaliteit is een alternatief voor Fast User Switching en werkt alleen in combinatie met Citrix of Terminal Services. De gebruiker start met het inloggen op het netwerk en het opstarten van de benodigde applicaties (de SSO-oplossing zorgt voor het automatisch inloggen). Als deze gebruiker van werkplek wisselt, dan heeft hij de mogelijkheid om de ingelogde sessie 'mee te nemen' naar een andere werkplek. De gebruiker heeft direct toegang tot de al eerder gestarte desktop met de openstaande applicaties. Net als bij Fast User Switching is het mogelijk om het wisselen van gebruikers te koppelen aan een gebruikerspas. Hierdoor hoeft een gebruiker zich alleen bekend te maken met een pasje en optioneel een pincode. Fast User Switching en Follow Me zijn functionaliteiten die binnen SSO beschikbaar zijn. Er is geen zware implementatie voor nodig.

Voor reacties en nieuwe bijdragen van deskundigen: Henk Ester (h.ester@sdu.nl, (070) 378 03 97).