Single Sign On
op basis van een digitaal certificaat

Het realiseren van een "Single Sign On" of "Reduced Sign On" scenario in een organisatie biedt grote kostenbesparingen, verminderd beheer en een beter beveiligingsniveau. Een sleutelpositie binnen een "Single Sign On" systeem wordt ingenomen door het digitale certificaat. Met een digitaal certificaat kan op het niveau van de infrastructuur de toegang tot een informatieverwerkend systeem geregeld worden. Hierdoor kunnen eenvoudige web toepassingen vrijwel naadloos gebruik maken van de diensten die een "Single Sign On" systeem biedt. Complexere systemen vereisen aanpassingen, deze zullen voornamelijk gericht zijn op het rechtenbeheer.

De klassieke opzet voor een informatieverwerkend systeem is zo dat authenticatie, autorisatie en registratie met het systeem verweven zijn. Het informatieverwerkende systeem heeft een authenticatiemechanisme, een registratiesysteem (bijvoorbeeld in de vorm van een database tabel) en een autorisatiesysteem. Over meerdere informatieverwerkende systemen worden telkens dezelfde gegevens (en vaak ook over dezelfde gebruikers) vastgelegd. Dit betekent dat er binnen een organisatie een enorme redundantie aan gegevens bestaat met alle nadelen die daar aan kleven zoals de beheerinspanning die geleverd moet worden op het in stand houden van de gebruikersregistraties. Daarnaast is er verlies van integriteit in de gegevens doordat verschillende organisatieonderdelen de gegevens bijhouden en het risico van inbreuk doordat gebruikers de vele wachtwoorden noteren en op hun werkplek laten rondslingeren.

> Authenticatie: het proces waarin vastgesteld wordt of de aangeboden identiteit juist is, bijvoorbeeld door het controleren van een wachtwoord.
>
> Autorisatie: het proces waarin rechten toegekend worden aan een gebruiker (of systeem) om een bepaalde functie uit te kunnen voeren of systeembronnen te benaderen.
>
> Registratie: de verzameling van gegevens die als uitgangspunt dient voor het nemen van authenticatie en autorisatie beslissingen.

De Giga Information Group[1] heeft uitgerekend dat bij een bedrijf van 20.000 medewerkers twintig procent van de helpdesk telefoongesprekken (3.000 gesprekken in totaal per maand) betrekking heeft op het opnieuw instellen van een wachtwoord. Elk incident kost tussen de 30 à 60 euro waardoor het totaal bedrag voor het bijhouden van gebruikersregistraties uitkomt op ruwweg 216.000 à 648.000 euro per jaar. De kosten voor het beheren van alle registraties en de schade die voortvloeit uit inbreuk van een informatieverwerkend systeem zijn in deze calculatie nog niet meegenomen.

Single Sign On

De oplossing hiervoor is "Single Sign On", ofwel "eenmalig inloggen". Gebruikers loggen maar een keer in en kunnen vervolgens alle deelnemende applicaties benaderen zonder opnieuw in te hoeven loggen. Volledige "Single Sign On" is in grote organisaties vaak moeilijk of slechts tegen zeer grote kosten haalbaar. Een alternatief is dan van een "Reduced Sign On" waarbij een aantal grote systemen en/of systemen die veel beheer vergen worden geschikt gemaakt voor een "Single Sign On" systeem terwijl een aantal kleinere of minder belangrijke informatieverwerkende systemen ongemoeid wordt gelaten. Hierdoor wordt een kostenreductie gerealiseerd zonder door te schieten en extra kosten uit te geven om alles onder een paraplu te krijgen. In het vervolg van dit artikel wordt uitsluitend gerefereerd aan de term "Single Sign On" om de technologie aan te duiden, niet het gewenste eindresultaat.

Om een "Single Sign On" scenario te kunnen realiseren moeten er drie zaken geregeld worden:

- Een gemeenschappelijke (gebruikers) registratie;
- Een transparant authenticatiemechanisme;
- Een standaard autorisatiemechanisme;

GEMEENSCHAPPELIJKE REGISTRATIE

De basis voor Single Sign On is een gemeenschappelijke gebruikersregistratie die de veelheid aan losse administraties vervangt. De gemeenschappelijke gebruikersregistratie wordt vaak

[1] IdeaByte™, "Password Reset Software Can Reduce Help Desk Costs," Giga Information Group.

gebaseerd op het concept van Directory Services. Een Directory Service is een hiërarchische object georiënteerde database met een standaard interface[2]. Gegevens worden opgeslagen in een boomstructuur waarbij de nadruk ligt op optimalisatie van lees operaties . Grote software leveranciers zoals Microsoft, Sun en IBM zijn al enige tijd bezig hun eigen software geschikt te maken voor de omgang met Directory Services. Met name Microsoft heeft veel impact gehad op deze markt door de introductie van Active Directory als centraal punt voor de opslag van gebruikersgegevens (en andersoortige informatie). De toegang tot de Directory Service wordt geboden op basis van een standaardprotocol dat onafhankelijk is van zowel het server- als het client platform. Vergelijkbare oplossingen zijn ook realiseerbaar op basis van andere technologieën zoals relationele databases met een generieke interface zoals bijvoorbeeld SOAP[3]

TRANSPARANTE AUTHENTICATIE

Een lastig onderdeel van Single Sign On is het realiseren van een standaard methode voor authenticatie die transparant is voor gebruikers. Transparantie vereist dat het gegeven dat de gebruiker succesvol ingelogd is ter beschikking gesteld wordt aan andere informatieverwerkende systemen. Het beschikbaar stellen van deze informatie dient op veilige wijze plaats te vinden omdat anders een veiligheidslek wordt gecreeerd. Er zijn verschillende methodes beschikbaar waarbij een onderscheid gemaakt kan worden tussen de webtechnologie en niet-webtechnologie benadering. In de laatste categorie valt Kerberos, een gedistribueerd beveiligingssysteem dat gebaseerd is op symmetrische encryptie. Kerberos is bedacht door MIT en vormt onder andere het hart van de Windows 2000 beveiligingsservices. In dit artikel zal uitsluitend ingegaan worden op de webtechnologie benadering waarbij twee exponenten te onderscheiden zijn.

De eenvoudigste manier om informatie over het succesvol inloggen ter beschikking te stellen binnen een omgeving die met web technologie werkt is via HTTP cookies[4]. Een web server kan authenticatie uitvoeren door de aangeboden identificatiegegevens te controleren in de centrale gebruikersregistratie. Als de authenticatie succesvol uitgevoerd wordt dan plaatst de web server een cookie op de werkplek van de gebruiker. Als de gebruiker vervolgens de diensten van een ander informatieverwerkend systeem benaderd wordt het gegenereerde cookie automatisch meegenomen in elk verzoek aan het andere systeem. Het authenticatiemechanisme van dit andere systeem detecteert het cookie, leest het uit en kan in de centrale gebruikersregistratie nagaan welke rechten de gebruiker heeft bij deze nieuwe applicatie. Er is geen noodzaak om nogmaals om authenticatie te vragen omdat de nieuwe applicatie via het cookie heeft doorgekregen dat dit al succesvol is uitgevoerd. Het is een eenvoudig systeem dat het hart vormt van het gros van de commerciële aanbiedingen voor "Single Sign On" oplossingen zoals Netegrity SiteMinder, IBM Policy Director of Baltimore SelectAccess. Er kleven echter wel veel nadelen aan, het cookie is beperkt tot een specifiek domein (bijvoorbeeld .more-secure.nl) en kan niet gebruikt worden door informatieverwerkende systemen in andere domeinen (bijvoorbeeld .not-secure.nl). Daarnaast is al enkele malen gebleken dat browsers fouten kunnen hebben die de inhoud van de lokale omgeving openbaren aan kwaadwillenden, waaronder dus ook cookies.

Een veiligere oplossing wordt geboden door gebruik te maken van de faciliteiten van het SSL[5] protocol. SSL is het defacto beveiligingsprotocol in de Internet wereld. Het wordt gebruikt voor het beveiligen van HTTP verkeer (web verkeer) maar het kan ook gebruikt worden voor andere protocollen zoals SMTP (mail), FTP (filetransfer) of Telnet (administratie op afstand). SSL versleutelt het verkeer tussen de client en de server waardoor het onleesbaar wordt voor onbevoegde gebruikers. Het basismateriaal voor de versleuteling wordt geleverd door digitale certificaten.

Digitale certificaten zijn gebaseerd op asymmetrische encryptie (zie tekstbox) en ze bevatten cryptografische sleutels die gebruikt kunnen worden om informatie te versleutelen. Digitale certificaten kunnen gebruikt worden aan de kant van de server en heten dan server certificaten.

[2] Het LDAP (Lightweight Directory Access Protocol) protocol.
[3] Simple Object Access Protocol.
[4] HTTP cookies zijn kleine tekstbestanden die op de werkplek van de gebruiker opgeslagen worden.
[5] Secure Sockets Layer. De door het IETF gestandaardiseerde versie staat bekend onde de naam TLS, Transport Layer Security.

Symmetrische encryptie: versleuteling gebaseerd op een gedeelde sleutel, dus zowel de verzender als de ontvanger gebruiken dezelfde sleutel.

Asymmetrische encryptie: de verzender en ontvanger maken elk gebruik van twee sleutels, een private sleutel die geheim gehouden wordt en een publieke sleutel die aan iedereen verspreid mag worden. De private sleutel wordt gebruikt voor het ontcijferen van berichten en digitale handtekeningen, de publieke sleutel wordt gebruikt voor versleutelen van berichten en de verificatie van digitale handtekeningen.

Server certificaten worden gebruikt om de identiteit van de server te bewijzen (gebaseerd op de URL van de server) en de verbinding te versleutelen. Digitale certificaten kunnen ook gebruikt worden aan de kant van de gebruiker en heten dan client certificaten. Client certificaten kunnen gebruikt worden om de identiteit van de gebruiker vast te stellen. Deze mogelijkheid komt goed van pas bij een "Single Sign On" oplossing. Zodra de server binnen de protocol onderhandelingen met de client vaststelt dat de client over een eigen certificaat beschikt wordt dit automatisch meegenomen in het onderhandelingsproces. De server weet van verzoek tot verzoek met wie er gecommuniceerd wordt en deze informatie wordt op een vele malen veiligere wijze overgedragen dan via cookies. De server kan op basis van een uniek kenmerk in het certificaat zoals gebruikersnaam of serienummer de bijbehorende gebruikersgegevens opzoeken in de centrale registratie. Als er een overeenkomstige gebruiker gevonden wordt dan is de gebruiker geauthenticeerd. Gaat de gebruiker naar een volgend informatieverwerkend systeem dan worden transparant voor de gebruiker dezelfde stappen herhaald. Dit heeft als voordeel dat tussentijdse wijzigingen in de status van de gebruiker van invloed kunnen zijn op het verloop van de authenticatie. Een gebruiker kan met een client certificaat alle informatieverwerkende systemen benaderen die de SSL onderhandeling kunnen uitvoeren en die toegang hebben tot de centrale gebruikersregistratie. In principe kan elke moderne web server deze handelingen uitvoeren waardoor de mogelijkheden voor "Single Sign On" op basis van digitale certificaten erg groot zijn.

STANDAARD AUTORISATIE

De laatste stap om het "Single Sign On" systeem compleet te maken is het standaard autorisatiemechanisme. Het autorisatiemechanisme zelf mag in principe van systeem tot systeem verschillen maar de methode van het verkrijgen van autorisatiegegevens dient gestandaardiseerd te zijn. Het autorisatiemechanisme zal uit de centrale registratie de applicatiefuncties op dienen te roepen die uitgevoerd mogen worden door de geauthenticeerde gebruiker. De selecterende sleutel om deze gegevens uit de centrale registratie op te roepen wordt verstrekt door het client certificaat in de vorm van een ingebed serienummer of gebruikersnaam. Het direct koppelen van een gebruiker op applicatiefuncties is echter een ongewenste zaak. Elke keer als er iets wijzigt in de applicatie (extra applicatiefuncties) of in de status van de gebruiker (andere werkzaamheden) moet de gebruikersregistratie gewijzigd worden. Door te gaan werken met groepen van applicatiefuncties en die groepen te modelleren op werkzaamheden van gebruikers kunnen rollen gecreëerd worden. Een rol is een vertaling van de werkzaamheden van een gebruiker binnen een bedrijfsproces naar applicatie functies. Door een gebruiker te koppelen aan een rol (of meerdere rollen) en de rol te koppelen aan de applicatiefuncties wordt bereikt dat wijzigingen in de status van de gebruiker (andere werkzaamheden) geen impact heeft op de applicatie functies (de gebruiker krijgt alleen een andere rol) en wijzigingen in de applicatiefuncties (extra functies) geen impact hebben op de gebruiker (de extra functies worden toegekend aan de rol). Deze aanpak staat bekend onder de term "Role Based Access Control".

CONCLUSIE

Door gebruik te maken van een centrale gebruikersregistratie en een standaard, transparant authenticatiemechanisme kan een groot gedeelte van het "Single Sign On" scenario ingevuld worden. Partijen zoals Microsoft bieden deze voorziening als onderdeel van het Netwerk Operating System maar ook binnen de Unix omgeving zijn deze voorzieningen ruimschoots aanwezig. Het toevoegen van een gestandardiseerd autorisatiemechanisme in de vorm van Role Based Access Control biedt meerwaarde op het gebied van beheer, beheersbaarheid en beveiliging. Een aantal leveranciers biedt hulpmiddelen voor het beheren van rollen binnen een centraal registra-

tiesysteem maar het zelf inrichten op basis van standaardcomponenten behoort ook tot de mogelijkheden. Voor kleine systemen met bescheiden behoeftes op het gebied van autorisatie kan een "Single Sign On" oplossing in korte tijd gerealiseerd worden. Complexere systemen met veel autorisatielagen vereisen meer werk maar kunnen ook profiteren van de kennis die er is opgebouwd binnen de "Role Based Access Control" aanpak.

MORE-SECURE

More-Secure kan u begeleiden in het ontwerpen van een passende "Single Sign On" architectuur, het maken van produktkeuzes en het implementeren van de gekozen oplossing.

Contact

More-Secure BV

Da Costalaan 14
3767GH Soest
T: +31 (0)6 5357 9338
F: +31 (0)35 524 7587
E: info@more-secure.nl
W: www.more-secure.nl