

In het kort:
 Goede integratie
 met Forefront
 Claims based
 authenticatie
 Form based
 authenticatie
 IPsec en SSL

Veiligheid in en om SharePoint

MAIK VAN DER GAAG EN GIJS IN 'T VELD

SharePoint inzetten zoals het door Microsoft is bedoeld, resulteert in een centrale gebruikersomgeving die op allerlei manieren kan worden benaderd. Dit stelt hoge eisen aan de veiligheid op alle fronten. Met de juiste keuzes en de tools uit dit artikel kunt u een uitstekend beveiligde SharePoint-omgeving opzetten.

Inleiding

Bij veel organisaties wordt SharePoint gebruikt voor het opslaan en delen van grote hoeveelheden data. Maar het delen van data betekent niet "toegankelijk maken voor iedereen", omdat de data vaak informatie bevat die niet zomaar met iedereen gedeeld mag worden, zoals bedrijfsgegevens en privacygevoelige gegevens. De combinatie van veiligheid en toegankelijkheid van de data is hierbij een interessante uitdaging met bovendien tegenstrijdige belangen.

Met de inzet van SharePoint is het van belang om op alle niveaus van de omgeving te letten op de veiligheid. Die niveaus zijn: Windows Server, IIS-Configuratie, ASP.NET-configuratie, SharePoint configuratie, communicatie- en firewall-configuratie.

Om ervoor te zorgen dat er een veilige omgeving ontstaat, maakt SharePoint gebruik van verschillende niveaus van het Microsoft Platform. Dit gebeurt met de volgende technieken:

- Authenticatie met windows-accounts
- SharePoint permissies-model
- Beheermogelijkheden code-accesssecurity
- Transportbeveiligingstechnieken zoals SSL en IPsec
- Transparent Database Encryption
- Firewall-bescherming

De gebieden waar veiligheid belangrijk is, zijn:

- Authenticatie (het identificeren van gebruikers)
- Autorisatie (wie mag wat met content doen)
- Communicatiebeveiliging (niemand mag data onderweg onderscheppen)
- Opslagbeveiliging (alles veilig opgeslagen)

Al deze gebieden komen in dit artikel aan de orde. Verder gaan we in op het belang van bepaalde beveiligingstechnieken in de verschillende SharePoint-topologiën en een aantal veelgebruikte tools om een veilige omgeving te creëren.

Authenticatie

Als u gebruikmaakt van SharePoint, hebt u de mogelijkheid om verschillende authenticatiemethoden toe te passen. Authenticatie binnen SharePoint is nodig om te kunnen monitoren wie wat doet en om de juiste rechten toe te kunnen kennen aan gebruikers. In de volgende alinea's worden kort en bondig de authenticatiemethoden beschreven die binnen SharePoint kunnen worden gebruikt.

Anonymous

Anonymous authenticatie geeft de gebruikers de mogelijkheid om informatie te vinden en bekijken op publieke gedeelten van een website. Het betekent dat de gebruiker geen inlogge-

vens nodig heeft om bepaalde gedeeltes van een website te bezoeken. Binnen SharePoint is het mogelijk om een website te creëren waarin een bepaald gedeelte anoniem toegankelijk is en een ander gedeelte niet.

Basic

Basic-authenticatie vereist dat u beschikt over een toegewezen windows-account. De authenticatiemethode verstuurt de accountgegevens tijdens een http-transactie. Dit wil zeggen dat de gegevens als tekst worden verstuurd. Het is daarom aanbevolen om met basic-authenticatie in combinatie met secure sockets layer (SSL) encryptie te gebruiken zodat gegevens versleuteld worden.

Digest

Digest-authenticatie is in principe dezelfde authenticatiemethode als basic-authenticatie. Het verschil is dat bij digest-authenticatie de accountgegevens versleuteld worden verstuurd.

Client-certificaten

Client-certificatenauthenticatie is een authenticatiemethode die kan worden gebruikt wanneer er gebruik wordt gemaakt van een SSL-verbinding tussen de clients en de webserver. Deze authenticatiemethode kan bijvoorbeeld worden gebruikt bij een extranet waarbij het veiligheidsbeleid twee niveaus vereist. Client-certificatenauthenticatie vereist dat clients een X.509-certificaat hebben en daarnaast hun authenticatiegegevens kunnen aanbieden.

Form-based authenticatie

Form-based authenticatie is een authenticatiemethode waarbij het mogelijk is een eigen identiteitmanagementsysteem dat is gebaseerd op ASP.NET-membership en rol-providers te gebruiken. In SharePoint 2010 is form-based authenticatie alleen beschikbaar wanneer u claims-based authenticatie gebruikt

NTLM

NTLM is de standaard windowsloginprocedure met een groot voordeel ten opzichte van andere

authenticatiemethoden. Dit is omdat voor het gebruik van deze authenticatiemethode geen extra instellingen gedaan hoeven te worden.

NTLM maakt gebruik van een challenge-responsemechanisme zoals in **Figuur 1** is weergegeven. Applicatieprotocollen maken gebruik van dit mechanisme om gebruikers te authenticeren. **Figuur 1** beschrijft hoe een gebruiker (client) geauthenticeerd wordt door een server die zich in het domein bevindt.

Kerberos

Kerberos is een netwerk authenticatieprotocol waarmee het mogelijk wordt computers te authenticeren. Eigenschappen van Kerberos-authenticatie zijn:

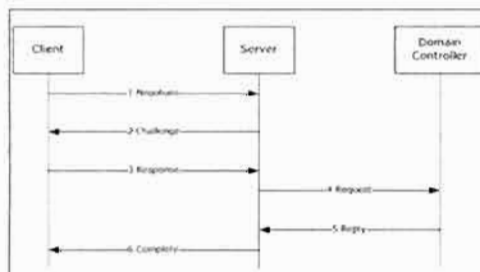
- Wederzijdse authenticatie tussen client en server
- Minimalisering van belasting van alle partijen
- Geen uitwisseling van wachtwoorden
- Naspelen van de authenticatie is niet mogelijk

Kerberos maakt gebruik van een vertrouwde partij voor de authenticatie; een key distribution center (KDC) dat bestaat uit twee delen: de authenticatieserver en de ticket-granting server. Voor de communicatie tussen twee entiteiten genereert de KDC een session-key die gebruikt kan worden om de communicatie over en weer te beveiligen.

Om zich te authenticeren, geeft een gebruiker zijn wachtwoord zodat hij kan aantonen wie hij is. De KDC geeft op basis van die gegevens een soort paspoort af, een ticket granting ticket (TGT). Met de TGT vraagt de Kerberos-client toegang aan voor services bij de KDC. Op basis van de TGT geeft de KDC een session-ticket voor de service. Met het session-ticket kan de client vervolgens de service benaderen voor toegang. Voor iedere service die de client wil benaderen moet een session-ticket worden gemaakt. De TGT en de session-ticket blijven lang geldig en kunnen meerdere keren worden gebruikt om de sessies op te bouwen. Dit minimaliseert de belasting van de KDC en de service.

In SharePoint 2007 is het noodzakelijk om Kerberos-authenticatie te gebruiken wanneer er gecommuniceerd moet worden met backend-systemen zoals Analysis Services en Reporting Services onder de accountgegevens van de huidige gebruiker.

Figuur 1
Authenticatie met NTLM.



Claims-based authenticatie

Met de komst van SharePoint 2010 is het nu ook mogelijk om claims-based authenticatie te gebruiken. Claims-based authenticatie maakt het mogelijk om vanuit meerdere identity stores (Active Directory, Live ID, ASP.Net Membership) een token te maken. Deze tokens worden gemaakt door een security token service (STS). Binnen SharePoint werkt dit ongeveer als volgt:

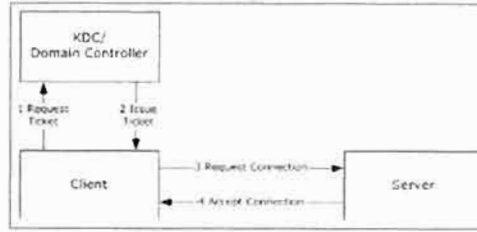
1. Er wordt een site opgevraagd en de SharePoint-applicatie vraagt of de gebruiker zich wil authenticeren. Daarnaast geeft SharePoint de URL terug van de STS omdat de gebruiker zich daar moet authenticeren.
2. De client vraagt om een token aan de identity-provider die behoort bij de STS. die SharePoint heeft aangewezen.
3. De identity-provider controleert de authenticiteit, genereert een token en stuurt deze terug naar de client.
4. De client stuurt de token naar SharePoint. SharePoint controleert de token met zijn eigen STS en vraagt vervolgens of er additionele informatie is van de gebruiker. Met deze informatie maakt SharePoint een nieuw token en stuurt deze naar client.
5. De client vraagt de pagina opnieuw op met daarbij het token. SharePoint weet nu wie de gebruiker is en zet het token om in een SPUser-object. Aan de hand van het object weet SharePoint of de gebruiker de juiste rechten heeft.

Omdat rechten gedelegeerd moeten worden om gebruik te maken van bijvoorbeeld het RSS-webpart in SharePoint, was het in SharePoint 2007 vereist om Kerberos te gebruiken. Met de komst van claims-based authenticatie in SharePoint 2010 is dit niet meer noodzakelijk. Een bijkomend voordeel is dat claims-based authenticatie in combinatie met forms-based authenticatie een naadloze integratie verzorgt met Office 2007 SP2 en Office 2010, iets wat in SharePoint 2007 ook niet mogelijk was.

Autorisatie

Autorisatie is de procedure waarmee rechten voor een persoon binnen een bepaald object worden geregeld. Binnen SharePoint kan de autorisatie op verschillende niveaus worden ingesteld. Op webapplicatieniveau moeten deze autorisaties gewijzigd worden door een farm-administrator. De administrator heeft de volgende mogelijkheden op web applicatieniveau:

- "Policy for web application": De administrator kan hier aangeven welke gebruiker



Figuur 2 Authenticatie met Kerberos.

- bijvoorbeeld "Full read" of "Full control" toestemmingen hebben. Het content accessaccount voor SharePoint search wordt hier automatisch geregistreerd met full-read toegang op de webapplicatie.
- "User permissions for web application": De administrator kan op webapplicatieniveau aangeven of een gebruiker bijvoorbeeld een site aan mag maken.

In SharePoint 2010 is er ook de mogelijkheid gebruikersrechten te geven op service-applicaties.

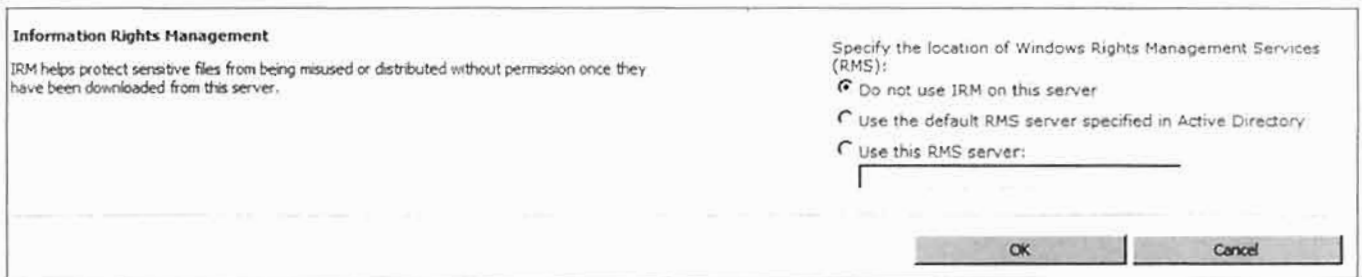
Site-collectionadministrators en site-owners kunnen daarnaast gebruikers rechten geven op sites, lijsten, folders en items. Deze rechten kunnen allemaal apart worden ingesteld. Naast deze rechten kunnen ze ook binnen een site site-groepen creëren waar bepaalde rechten aan worden toegekend.

Information Rights Management (IRM)

Information Rights Management is een oplossing waarmee u de toegang tot inhoud van documenten, werkmappen en presentaties kunt beperken en beveiligen. Hierbij kan bijvoorbeeld worden gedacht aan het toevoegen van een houdbaarheidsdatum aan een document of het onmogelijk maken van afdrucken of screenshots maken.



Figuur 3 Het beheerscherf van de Secure Store Service.



Figuur 4 De IRM-services instellingen.

Voordat er gebruikgemaakt kan worden van IRM voor lijsten en bibliotheken moet er een aantal services worden geïnstalleerd en geconfigureerd:

- Op elke front-end in de farm moet Windows Rights Management Services Client worden geïnstalleerd en IRM-protectors voor de bestandstypes die met IRM beveiligd gaan worden.
- In Central Administration moet IRM zijn ingeschakeld.

Met IRM kunnen verschillende machtigingen worden ingesteld. Voorbeelden hiervan zijn:

- Machtiging om te printen: De gebruiker moet hiervoor wel leesrechten of hogere rechten te hebben.
- Machtiging om Microsoft Visual Basic for Applications, scripts en andere programmacode in het bestand te voegen.
- Het aantal dagen dat het document geldig is. Is de ingestelde tijd verstreken, dan moet de gebruiker het document opnieuw downloaden.
- Machtiging die gebruikers toestaan filetypen te uploaden die niet worden gesupport door IRM.
- Optioneel: het opheffen van de IRM-rechten op de documenten na een bepaalde datum.

Code Access Security

SharePoint maakt gebruik van codeaccess-security om toegang tot beveiligde informatie te beheren. Codeaccess-security is een beveiligingsmechanisme dat de mogelijkheid biedt om SharePoint onder een beveiligingsniveau te draaien dat is geselecteerd uit een voor-gedefinieerde set van toestemmingen.

Met deze gedefinieerde toestemmingen kan worden ingesteld of bepaalde code wordt vertrouwd op een bepaald niveau, afhankelijk van waar de code vandaan komt en afhankelijk van de identiteit van de persoon. Met het definiëren van toestemmingen voor code access security worden de volgende mogelijkheden gecreëerd:

- Definiëren van rechten voor toegang tot system-resources.
- Administrators de mogelijkheid geven om veiligheidsbeleid te associëren met code.
- Specificeren wat code wel en niet mag uitvoeren.

- Toestemmingen toekennen aan alle assemblies die worden geladen door de applicatie.
- Een certificaat bezitten vereisen van alle personen die de code uitvoeren. Dit zorgt ervoor dat u zeker bent dat de persoon die de code uitvoert iemand uit de eigen organisatie is.

Om administrators de mogelijkheid te geven te wisselen tussen verschillende levels is er een aantal standaard security-policies:

- Windows SharePoint Services Minimal (WSS_Minimal)
- Windows SharePoint Services Medium (WSS_Medium)

Natuurlijk heeft de administrator ook de mogelijkheid om de beveiliging te negeren en de security-policy WSS_Full toe te voegen. Dit is zoals u begrijpt geen best-practice.

Communicatiebeveiliging

Het opzetten van beveiligde communicatie tussen componenten van een SharePoint-omgeving is een van de belangrijkste stappen om de veiligheid te garanderen. De beveiligde communicatie tussen de verschillende componenten draagt zorg voor de privacy en integriteit van datatransport en dataopslag binnen SharePoint.

Privacy wil zeggen dat documenten binnen de organisatie privé en vertrouwelijk blijven. Daarnaast is er de integriteit om ervoor te zorgen dat de documenten tijdens het opslaan en uploaden niet kunnen worden verminkt of aangepast.

Secure Sockets Layer (SSL)

SSL is een protocol dat veel wordt gebruikt om de communicatie tussen de browser en de webserver te beveiligen. Dit protocol kan met cryptografie zowel een beveiligde authenticatie verzorgen als een beveiligde verbinding maken over het internet. Het protocol zorgt ervoor dat af luisteren onmogelijk wordt. In SharePoint is het configureren van SSL eenvoudig te activeren door het zetten van een vinkje bij het creëren van een webapplicatie. Daarbij moet er natuurlijk wel worden beseft dat poort 443

wordt gebruikt door dit protocol. Binnen IIS dient daarnaast een certificaat van een Trusted Certificate Authority gekoppeld te zijn.

SSL werkt als volgt:

1. Een connectie wordt gemaakt en er wordt gecontroleerd of het certificaat van de website is uitgegeven door een certificaatleverancier die als vertrouwd te boek staat. De server stuurt daarnaast zijn public-key voor de encryptie naar de client.
2. De client en de server onderhandelen over welk algoritme wordt gebruikt voor de encryptie en de client stuurt zijn public-key naar de server.
3. De pakketten die vervolgens over en weer worden verstuurd, worden versleuteld en ontcijferd met de public-key van de ontvangende partij.

Internet Protocol Security (IPsec)

IPsec is een beveiligde communicatieoplossing die gebruikt kan worden om verkeer tussen verschillende componenten binnen een netwerk te beveiligen. Het maakt gebruik van een transportmechanisme waarmee de integriteit en vertrouwelijkheid van TCP/IP gebaseerd verkeer worden gewaarborgd.

Het basisprincipe van IPsec is het volgende. Al het verkeer tussen clients (geïnitieerd door applicaties, services, etc.) wordt volledig versleuteld door IPsec. IPsec markeert met eigen headers de pakketten die over de lijn worden verstuurd waardoor de ontvangende partij weet dat de pakketten ontcijferd moeten worden. Omdat al het verkeer is versleuteld, wordt voorkomen dat het verkeer kan worden afgeluisterd.

Het verschil tussen IPsec en SSL is dat bij SSL de applicaties die worden gebruikt afweten van het bestaan van de encryptie. Dit is niet het geval bij IPsec. Bij SSL wordt het verkeer op applicatie-niveau versleuteld en bij IPsec al het netwerkverkeer.

SQL-server

SharePoint is zeer afhankelijk van SQL-server. Bijna alles wat door SharePoint wordt opgeslagen, komt in een SQL-server database terecht. Een veilige SQL-serveromgeving is dus belangrijk. Naast alle beveiligmogelijkheden die hierboven zijn besproken, moet er dus worden gekeken naar de beveiliging van SQL-server.

Transparent Data Encryption

Met de komst van SQL Server 2008 is het ook mogelijk om gebruik te maken van Transparent

Data Encryption (TDE). Deze functionaliteit is alleen beschikbaar in de Enterprise Editie.

Het grootste voordeel van Transparent Database Encryptie is dat de encryptie methode volledig transparant is voor applicaties en services die van SQL gebruikmaken. Daarom kan hij ook probleemloos onder SharePoint worden ingezet. SharePoint merkt niet dat de database versleuteld is en praat zoals gewoonlijk met SQL, terwijl SQL intern de encryptie en ontcijfering verzorgt.

Wanneer Transparent Database Encryptie wordt aangezet, wordt alle data versleuteld. Denk hierbij aan log files, informatie in TempDB, snapshots, backups, enzovoort. Omdat de backups ook worden versleuteld en de encryptie-key niet aanwezig is op andere database-servers, is het niet zondermeer mogelijk backups terug te zetten op andere servers.

TDE voert de I/O-encryptie en decryptie realtime op van de data en de log bestanden. De encryptie maakt gebruik van een database-encryptie key (DEK), die wordt opgeslagen in de master database. TDE biedt de mogelijkheid om te voldoen aan een groot aantal wetten en voorschriften dat bestaat binnen verschillende industrieën. Developers kunnen dankzij TDE data versleutelen met AES- en 3DES-encryptiealgoritmen zonder bestaande applicaties aan te passen.

SharePoint-topologiën

Extranet

Een extranet is een website of SharePoint-site die gedeeltelijk over het internet beschikbaar wordt gesteld voor mensen buiten de organisatie. Omdat een extranet naar buiten openstaat, is de informatie beschikbaar buiten de muren van het kantoor. Daarom moet ervoor worden gezorgd dat deze omgeving goed beveiligd is. Er kunnen immers bedrijfskritische informatie en vertrouwelijke gegevens staan.

Om voor het juiste beveiligingsniveau te zorgen, kunnen de volgende stappen worden ondernomen:

- Opzetten Firewall Server, zoals de Forefront Threat Management Gateway (TMG).
- Encryptie van het verkeer met SSL.
- Form Based Authentication (FBA).

Of de beveiliging nog verder kan worden aangescherpt in een omgeving, hangt af van het type informatie dat wordt opgeslagen binnen SharePoint.

Internet

Onver het internet wordt tegenwoordig veelvuldig gebruikgemaakt van SharePoint omdat het een content-management systeem dat eenvoudig is in te richten en te onderhouden. Wanneer er voor SharePoint wordt gekozen, maakt men vaak gebruik van anonymous-authenticatie zodat de site algemeen toegankelijk is. Om gegevens te kunnen aanpassen, kan naast anonymous-authenticatie gebruik worden gemaakt van FBA.

Wanneer u gebruikmaakt van anonieme toegang, is het ook verstandig om sites in een zogenoemde lock-down modus te draaien. Dit betekent dat de ViewFormsPagesLock-down-feature geactiveerd moet worden (die zorgt ervoor dat gebruikers niet meer op een AllItems.aspx-pagina terecht kunnen komen). Mochten zij hier toch direct heen navigeren, dan wordt er gevraagd om inlog-gegevens. Om daarnaast de overige infrastructuur te beveiligen, is het zinnig te overwegen gebruik te maken van van Forefront Threat Management Gateway waarmee directe toegang tot de web-server kan worden geblokkeerd.

Tooling

Forefront-protection for SharePoint

Forefront-protection for SharePoint is de beveiligingstool van Microsoft dat op verschillende versies van SharePoint kan worden gebruikt. Een voordeel van Forefront, is dat het gemakkelijk integreert met SharePoint. Dit kan plaatsvinden door Forefront te installeren in de front-end en deze te configureren in SharePoint.

Forefront-protection for SharePoint levert de volgende functionaliteiten:

- Antivirus scanning.
- Keyword filtering.
- Extensie filtering.

Voor het scannen van documenten op virussen gebruikt Forefront de engines die u selecteert, waaronder VirusBuster, Sophos, Norman, Microsoft Anti Malware, Kaspersky, CA VET, CA Inoculate, Authentium Command en AhnLab. Forefront scant de documenten voordat ze worden opgeslagen onder andere op worms, schadelijke code en virussen.

De multi-engine aanpak van Forefront zorgt ervoor dat er verschillende virusdefinities en updates kunnen worden gebruikt voor het scannen van de documenten. Binnen Forefront kan worden aangegeven welke en hoeveel engines worden

gebruikt voor het scannen van de documenten. Naast het scannen van documenten hebt u met Forefront ook de mogelijkheid tot het blokkeren van bepaalde extensies en keyword-filtering. Om meerdere Forefront servers te beheren, kan er gebruik worden gemaakt van Forefront Server Security Manager Console (FSSMC).

Forefront Threat Management Gateway

Forefront Threat Management Gateway is de volgende generatie versie van ISA-Server 2006 en is een geavanceerde firewall en webcache oplossing voor de betere beveiliging van een netwerk. Wanneer er gebruik wordt gemaakt van Forefront Threat Management Gateway, heeft het internet niet direct toegang tot de servers die zich achter de Forefront Threat Management Gateway server bevinden (omdat connecties die binnenkomen op de Forefront Threat Management Gateway Server worden doorgestuurd naar de juiste server).

Conclusie

Met SharePoint en de andere besproken tools van Microsoft kunt u binnen en rond SharePoint veel aan de beveiliging doen. Welke beveiligingsstappen u kunt nemen, ligt aan de structuur en het type omgeving dat wordt opgezet. Als de omgeving toegankelijk is vanaf het internet, zal er een strakkere beveiliging moeten zijn dan wanneer de omgeving alleen intern benaderbaar is. Daarnaast vormen virus- en malware-scanners zoals Forefront altijd een toegevoegde waarde voor een omgeving. Hiermee wordt voorkomen dat er iets wordt geüpload met virussen, malware, niet legale content of een mp3-bestand waarop auteursrechten rusten. Veiligheid moet al de volle aandacht hebben bij het uitdenken van een SharePoint-architectuur. Door de juiste keuzes te maken en de in dit artikel genoemde technieken en tools toe te passen, kan een uitstekend beveiligde SharePoint-omgeving worden opgezet. ■

MAIK VAN DER GAAG (maik.vandergaag@motion10.com, <http://msftplayground.com>) is SharePoint Consultant bij business integration specialist motion10 en zaalvoetballer. Maik is sinds 2007 gespecialiseerd in het ontwikkelen van SharePoint oplossingen.

GIJS IN 'T VELD (gijs.intveld@motion10.com), MVP, is CTO bij motion10 waar hij onder andere verantwoordelijk is voor de technologische visie en strategie.