Secure Development bij verzekeraar Achmea

Achterdeur in beveiliging IT-omgeving stevig op slot

Phons Stokkermans

De beveiliging van de informatievoorziening en van gevoelige informatie is voor Achmea erg belangrijk. De klant vertrouwt daarop en dat vertrouwen mag de verzekeraar niet schaden. Daarom heeft Achmea een beveiligingsnorm voor systeemontwikkeling opgesteld. Door op deze norm te controleren is een ontwikkelteam verplicht om de juiste deliverables op te leveren. Om een ontwikkelteam hierbij te helpen wordt de Microsoft Security Development Lifecycle geïmplementeerd.

De afgelopen jaren is er veel aandacht besteed aan de beveiliging van de infrastructuur. Dankzij firewalloplossingen en antivirussoftware zit bij de meeste IT-omgevingen de voordeur wel op slot. Daarom richten hackers zich steeds vaker op de achterdeuren, de applicaties. Het is dus van groot belang dat bij het ontwikkelen van applicaties maatregelen getroffen worden om misbruik te beperken. Applicatiebeveiliging dient vanaf het begin van het ontwikkeltraject aandacht te krijgen. Hoe eerder een security bug gevonden wordt, des te goedkoper is het om deze te herstellen.

OWASP Top 10

Het Open Web Application Security Project (OWASP) is een gratis wereldwijde open community die zich richt op het verbeteren van de beveiliging van applicatiesoftware. Deze community heeft een top tien samengesteld van de meest voorkomende kwetsbaarheden in een webserver of webapplicatie. Achmea wil dat al haar internet- en intrane applicaties bestand zijn tegen de bedreigingen van de OWASP top tien. Om dit te kunnen borgen in het ontwikkelproces heeft Achmea in projectvorm, samen met Microsoft, de Microsoft Security Development Lifecycle (SDL) ingevoerd.

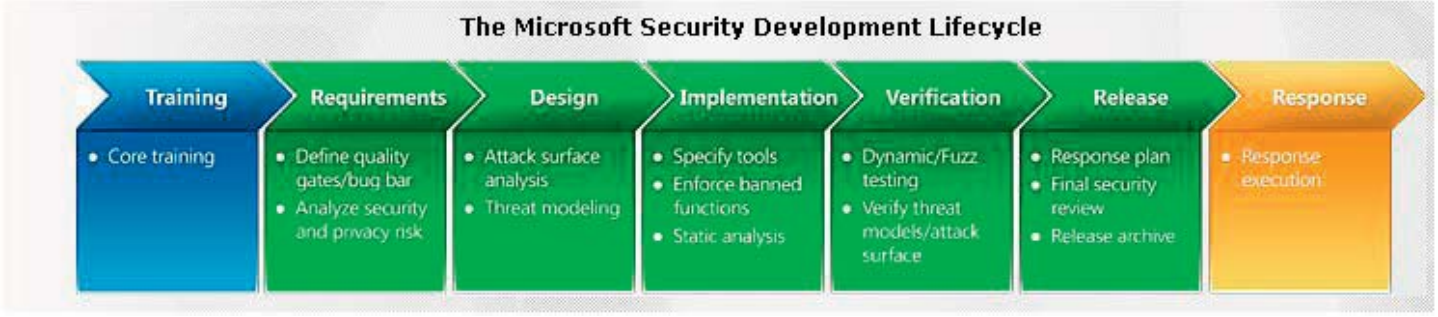
De Security Development Lifecycle is ontstaan uit het 'Microsoft thrustworthy computing' initiatief. Microsoft wilde met dit initiatief tegemoet komen aan de wensen van haar klanten om veiligere software te leveren en haar geloofwaardigheid als softwareleverancier behouden.

SDL voegt maatregelen en controlepunten aan een bestaand ontwikkelproces toe, waardoor de kwaliteit van de software verbeterd wordt. Dit wordt gerealiseerd door het verminderen van het aantal onvolkomenheden op het gebied van applicatiebeveiliging.

Bij de invoering maakt het project gebruik van het SDL Optimization Model. Dit model is ontworpen om op een consistente en kostenefficiënte wijze de Security Development Lifecycle te implementeren. Het model is onderverdeeld in vijf categorieën die gerelateerd zijn aan het softwareontwikkelproces: training , requirements en design, implementatie, verificatie en release en response. Het onderkent vier volwassenheidsniveaus voor het uitoefenen van deze categorieën. Na het vaststellen van het huidige volwassenheidsniveau van het ontwikkelproces in een organisatie wordt bepaald wat het gewenste volwassenheidsniveau is en wat de stappen zijn om dit niveau te bereiken.

Het uitvoeren van een goed ontwikkelproces is een combinatie van drie factoren: mensen, processen en techniek. Bij de implementatie van de Security Development Lifecycle bij Achmea, hebben we daarom aandacht aan deze factoren besteed.

FIGUUR 1: SECURITY DEVELOPMENT LIFECYCLE.



Mensen

De mens blijft de sleutel in het applicatiebeveiligingproces. Daarom is het uitgangspunt bij het invoeren van security development bij Achmea de medewerker geweest. Management commitment en het creëren van bewustzijn voor applicatiebeveiliging is de basis voor een succesvolle implementatie.
Er zijn voor het management security awareness presentaties gehouden en krijgt iedereen die bij het ontwikkelproces betrokken is, bijvoorbeeld architecten, ontwikkelaars, testers en projectleiders, een e-learning module aangeboden. In deze module wordt uitgelegd waarom applicatiebeveiliging voor Achmea belangrijk is en wat de consequenties zijn als dit niet goed gebeurt. Om projecten te helpen worden zogenaamde security adviseurs opgeleid. Deze consultants zijn onafhankelijk van het project. Na het volgen van een diepgaande security Masterclass zijn zij in staat om kennissessies, hands-on hulp en advies aan projecten te geven, bijvoorbeeld op het gebied van applicatiearchitectuur, code of testen. Ook bewaken zij dat projecten voldoen aan de opgestelde standaarden en beveiligingsrichtlijnen.

Processen

Het ontwikkelproces van .NET applicaties bij Achmea moet aan een aantal kwaliteitseisen voldoen.
Daarom moet een minimale set aan deliverables door elk ontwikkelproject opgeleverd worden. In het bestaande proces werd al aandacht aan applicatiebeveiliging besteed. In de analysefase, wordt samen met de business een zogenaamde SPRINT analyse uitgevoerd. Hiermee wordt het risico van de applicatie voor de organisatie op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid bepaald. De applicatie krijgt een zogenaamde BIV classificatie. In het Project Start Architectuur document wordt deze BIV code met andere non-functional requirements opgenomen. Zo is bij het begin van het ontwikkeltraject al bekend aan welke kwaliteitseisen de applicatie moet voldoen.
Op 1 juni 2009 heeft Microsoft versie 4.1 van de SDL Process Guidance gepubliceerd. Hierin worden onder andere de standaarden en best practices voor beveiliging en privacy voor Line of Business applicaties beschreven. Deze SDL-LOB zorgt er voor dat de impact van de implementatie voor ontwikkelaars minimaal is. Het beschrijft per SDL fase een aantal high level security taken.

Training	Requirements	Design	Implementation	Verification	Release
LOB-specific training	Risk assessment • Application portfolio • Application risk assessment • Determine service level	Asset-centric threat modeling • Threat model • Design review	Internal review • Incorporate security checklists and standards • Conduct "self" code review • Security code analysis	Pre-production assessment • Comprehensive security Assessment • Bug tracking	Post-production assessment • Host level scan

FIGUUR 2: SECURITY DEVELOPMENT LIFECYCLE FOR LINE OF BUSINESS APPLICATIONS.

Aan het bestaande ontwikkelproces is een aantal Quality Gates toegevoegd. Door deze Quality Gates wordt aangetoond dat de applicaties voldoen aan de beveiligingsnorm van Achmea. Om de acceptatiegraad te vergroten, is veel aandacht aan de impact voor ontwikkelteams besteed. Deze impact is, zoals eerder aangegeven, minimaal gehouden.
Tijdens de designfase wordt een threatmodel van de applicatie gemaakt. Threat modeling is een systematisch proces waarmee zowel de bedreigingen en kwetsbaarheden in software alsook de tegenmaatregelen worden vastgesteld. De resultaten van dit proces worden opgenomen in de security view van het Software Architectuur Document.

Naast het beschrijven van use cases worden voortaan misuse cases gemaakt. Misuse cases zijn het tegenovergestelde van use cases en deze beschrijven ongewenst gebruik van het systeem. De actors uit de use cases worden nu mis-actors genoemd en zijn in het algemeen de aanvallers. Er moet ook rekening worden gehouden met onopzettelijke handelingen van goedaardige gebruikers. Voor de uitvoering van de misuse cases moeten de bedreigingen uit het threatmodel gehanteerd worden.
Aan de minimale set van deliverables is de misuse-case template toegevoegd.
Om veilige applicaties te bouwen moet voldaan worden aan secure coding standaarden. Het project heeft een reference card (Excel spreadsheet), waarin alle checks met betrekking tot Line of Business applicaties opgenomen zijn, opgeleverd. De basis voor deze spreadsheet zijn de checklists op MSDN. Per check wordt aangeven waarop deze betrekking heeft (Analysis & Design, ASP .NET, Webservices, WCF en Data Access). Bovendien wordt aangegeven op welke fase van SDL de check betrekking heeft en wat de tegenmaatregelen (mitigations) zijn. Hierop zijn filters aangebracht zodat de ontwikkelaar op eenvoudige wijze een overzicht met relevante informatie voor de betreffende situatie kan maken. Per check is een link met een verwijzing naar de uitleg met code voorbeelden opgenomen.
Naast de secure code standaard stellen we ook een handleiding voor het code review proces beschikbaar.
Voordat een applicatie in productie wordt genomen, wordt door een security-adviseur een zogenaamd Final Security Review uitgevoerd. Op basis van een template wordt getoetst of aan alle securitystandaarden en -richtlijnen en de voor de BIV code geldende bug bar is voldaan. De bug bar is het minimale kwaliteitsniveau waar de applicatie moet voldoen. Ook wordt gecontroleerd of alle deliverables zijn opgeleverd en of deze de status goedgekeurd hebben.

FIGUUR 3: SDL BEST PRACTICES EN DELIVERABLES @ ACHMEA.

Technologie

Team Foundation Server

Tooling die het proces goed ondersteunt, is belangrijk om een nieuwe werkwijze in een organisatie te laten landen. De .NET ontwikkelstraat van Achmea is gebaseerd op Visual Studio Team System. De wijzigingen met betrekking tot secure development moeten dus integreren met de bestaande tooling.

In juni heeft Microsoft de SDL Process Guidance Template voor Team Foundation Server beschikbaar gesteld. Deze template

helpt bij het toepassen van SDL in projecten. We hebben deze template bekeken en besloten onderdelen hiervan te gebruiken.

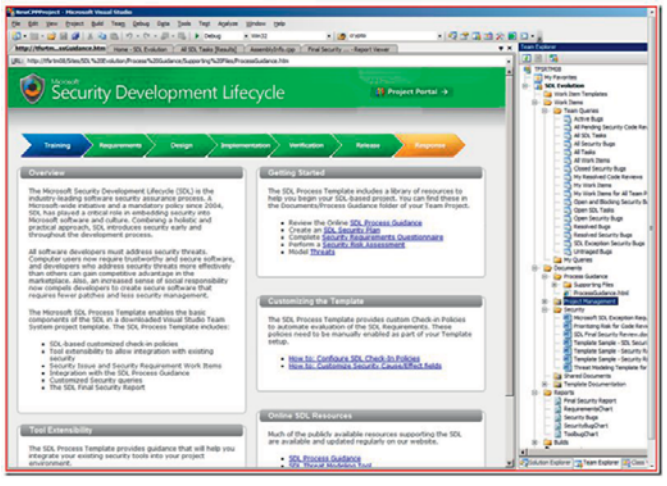
De redenen hiervoor zijn:

1. De template integreert niet met de MSF CMMi process template waarmee onze Team Projecten zijn aangemaakt. Ze is dus eigenlijk alleen geschikt voor nieuwe Team Projecten. We hebben delen van de template in onze bestaande team projecten geïmplementeerd.
2. De template genereert 93 SDL work items. Deze workitems zijn voor ons te gedetailleerd en we hebben een hebben een spreadsheet met 28 workitems gemaakt. Deze is gebaseerd op de minimale set aan deliverabels waarin SDL is opgenomen. De set met workitems kan eenvoudig in Team Foundation Server worden geïmporteerd.
3. Het onderdeel security in het workitem bug is erg uitgebreid. Ontwikkelaars en testers van LOB applicaties zullen moeite hebben met de keuze uit de vele opties van de SDL template. Wij hebben aan het workitem bug een veld security toegevoegd. Dit veld kan de volgende waarde bevatten: none (default), high, medium en low. Hierdoor zijn we in staat om met een zelf gemaakt rapport inzicht te krijgen in de hoeveelheid security bugs van de applicatie.

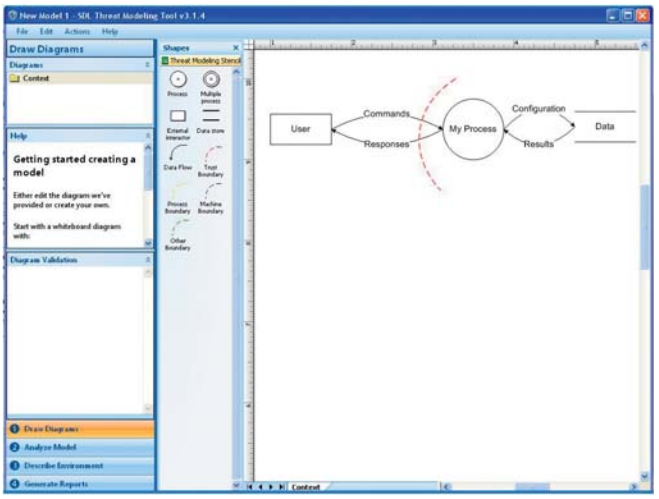
Microsoft heeft aangekondigd dat in de toekomst de concepten van de SDL template geïntegreerd zullen worden in de MSF agile proces template. Kijk voor meer informatie hierover op de blog van Brian Harry of de SDL blog op MSDN.

SDL Threat Model Tool

Om het threat modeling process te ondersteunen heeft Microsoft het SDL Threat Model Tool beschikbaar gesteld. Hiermee kan op eenvoudige wijze een Threat Model gemaakt worden.
Op basis van de Use case wordt een threat model van de applicatie gemaakt. Het tool analyseert en valideert het model en geeft aan wat de maatregelen zijn die getroffen moeten worden. Als alle stappen doorlopen zijn, dan kan een report van het model gegenereerd worden. Dit model bevat de informatie voor de security view van het Software Architecture Document.
Omdat 80% van de internet en intranet applicaties van Achmea dezelfde architectuur hebben, heeft het project een SDL template voor Achmea applicaties opgesteld. Met behulp van deze template is het opstellen voor een project specifiek threat model snel en eenvoudig te realiseren. Alleen van de onderdelen die afwijken van de referentie applicatie, moet nog een threat model gemaakt te worden.



FIGUUR 4: DE OPENINGSPAGINA VAN DE SDL PROCESS GUIDANCE.



FIGUUR 5: SDL THREAT MODEL TOOL MET DEFAULT DATA FLOW DIAGRAM.

Static Analysis

De projecten van Achmea moeten aan een vastgestelde set Static Analysis rules voldoen. Deze vastgestelde set bevat onder andere alle regels die betrekking op security hebben. Dagelijks worden de projecten in het daily build proces gebouwd en worden de Static Analysis rapportages opgeleverd.

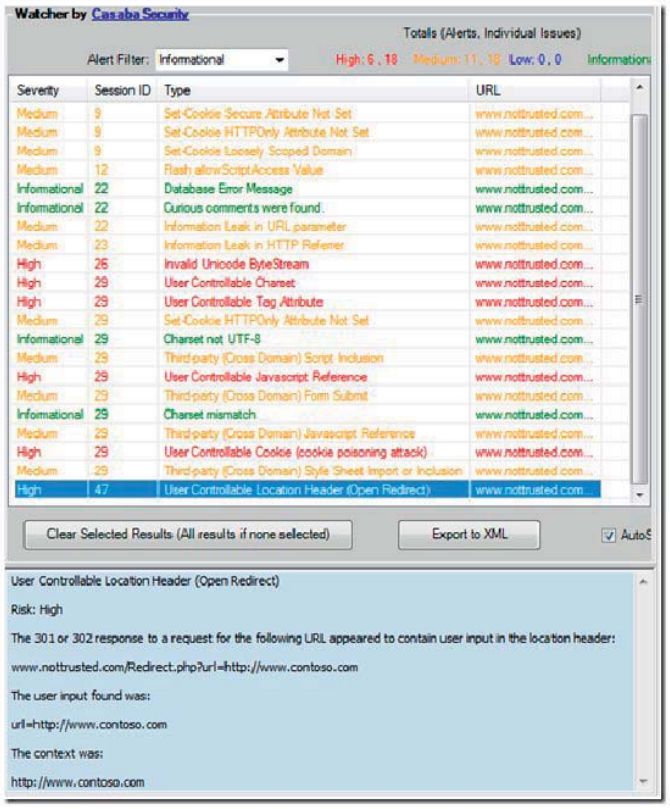
Security Testing Tool

Achmea wil ontwikkelaars en testers ondersteunen zodat zij veilige webapplicaties kunnen bouwen. Ook wil Achmea bij de productie acceptatie test toetsen of de applicatie bestand is tegen de bedreigingen van de OWASP top 10. Om dit te bereiken zal extra tooling worden ingezet. Gedacht wordt aan een commercieel product voor automatisch security testing en aan het web security testing tool van Casaba Security: Watcher. Watcher is een passief runtime analyse tool voor http-based web applicaties, dat controleert op bedreigingen in de OWASP top 10 en op configuratie settings. Met behulp van Watcher kunnen ontwikkelaars controleren of hun applicatie veilig is. Bovendien kunnen met Watcher penetratietests en audits uitgevoerd worden. Bij een penetratietest worden aanvallen van hackers gesimuleerd en wordt getoetst of de applicatie deze aanvallen kan pareren.
Watcher controleert onder andere de Silverlight clientaccesspolicy.xml en de configuratiesettings van SharePoint servers.
Wachter is een plug-in voor de Fiddler http debugging proxy. Hiermee kan de communicatie tussen de browser en de website gevolgd worden. Op de MSDN SDL Blog wordt lovend gesproken over Watcher. Het SDL team onderzoekt de mogelijkheid om Wachter als een aanbeveling op te nemen in een volgende versie van de Security Development Lifecycle.

Conclusie

Zoals gememoreerd, heeft het project gebruik gemaakt van het SDL Optimization Model.
Dit model kent vier volwassenheidsniveaus.

Bij de Start van het project is een nulmeting uitgevoerd en had Achmea het niveau Basic.
Bij afronding van het project zullen bijna alle onderdelen het volwassenheidsniveau Advanced bereikt hebben. Ook het doel, om webapplicaties bestendig te maken tegen bedreigingen van de OWASP Top 10, is bereikt.



FIGUUR 6: VOORBEELD RAPPORT VAN WATCHER.

FIGUUR 7: HET SDL OPTIMIZATION MODEL.

Door de invoering van de Security Development Lifecycle is Achmea in staat om aan te tonen dat haar webapplicaties aan de gestelde beveiligingseisen voldoen en dat voelt 'ontzorgt'

Links

Blog Brian Harry: http://blogs.msdn.com/bharry/
Fiddler http debugging proxy: www.fiddlertool.com
SDL blog: http://blogs.msdn.com/sdl/
OWASP: http://www.owasp.org/index.php/Main_Page
P&P Security checklists: http://msdn.microsoft.com/en-us/library/ms998392.aspx
SDL: http://msdn.microsoft.com/en-us/security/cc448177.aspx
SDL Tooling: http://msdn.microsoft.com/en-us/security/cc421514.aspx
SDL Optimization Model: http://msdn.microsoft.com/en-us/security/dd221356.aspx
Watcher Web security testing tool: http://websecuritytool.codeplex.com/

Phons Stokkermans, is Solutions Architect in het Microsoft Center of Excellence van Achmea.