BEST PRACTICES VOOR OPDRACHTGEVERS VOOR VEILIGE IT

Grip op Secure Software Development

Grip op Secure Software Development **is een verzameling richtlijnen over samenwerken voor goed beveiligde software. Het is een co-productie van tientallen specialisten, opdrachtgevers en leveranciers, onder de paraplu van het CIP: het *Centrum voor Informatiebeveiliging en Privacybescherming*.**

De richtlijnen gaan over samenwerking tussen opdrachtgever en software-ontwikkelaar en beschrijven duidelijke en meetbare beveiligingseisen. Deze publicaties zijn vrij beschikbaar op www.gripopssd.org en worden onderhouden door meer dan 20 organisaties in de groep 'Practitioners Grip op SSD', met Capgemini, IBM, UWV, Postnl, CIBG, Dictu, Belastingdienst, SVB, Binnenlandse Zaken, OWASP, CGI, Sogeti, Ordina, Software Improvement Group, DKTP en Valori. Naast de richtlijnen zijn ook trainingsmaterialen, testmethodes en inkoopcontracten voor vrij gebruik beschikbaar.

Het bijzondere van deze samenwerking is dat betrokken organisaties een manifest tekenen waarin ze zeggen te staan achter de Grip op SSD richtlijnen met de belangrijke opmerking dat daarvan kan worden afgeweken - mits dat wordt toegelicht aan de groep. Het zijn juist die afwijkingen die interessant zijn om te gebruiken als uitbreiding en verbetering van de richtlijnen. Dit resulteert in het delen van kennis en ervaring, zoals bijvoorbeeld de Cloud Security Alliance die helpt om security-aspecten specifiek voor de cloud toe te voegen. De richtlijnen zijn dus geen keurslijf, maar een communicatiemiddel en de betrokkenheid van zoveel partijen zorgt voor duurzame doorontwikkeling.

Door de samenwerking hoeven organisaties niet meer zelf het wiel uit te vinden wat betreft afspraken maken, contracten en beheersingsprocessen. Leveranciers vinden het ook prettig dat ze een standaard manier van werken hebben met meerdere van hun klanten.

Ontstaan van Grip op SSD

In mijn werk voor de Software Improvement Group (SIG) help ik organisaties met vraagstukken over softwarekwaliteit. Is een systeem onderhoudbaar? Schaalt het? Ook word ik gevraagd te kijken of security goed is ingebouwd en dan valt op dat hier de meest elementaire fouten worden gemaakt. SIG meet software security op een schaal van 1 tot 5 sterren en wat we veel zien zijn systemen die twee sterren scoren. Bij nader onderzoek blijkt dat dit vooral wordt veroorzaakt door onduidelijke afspraken en het gebrek aan een goede toetsing. Veel organisaties willen hier iets aan doen en zijn op zoek naar goede manieren om te regelen dat software veiliger wordt.

"Goed om aan het begin van het ontwikkeltraject een normenkader te hebben waarin security goed geborgd is."

Dion Kottemon
Oud-CIO Rijksoverheid

Over dit onderwerp raakte ik begin 2013 vanuit SIG in gesprek met het CIP. We wilden iets doen aan dit probleem en we zagen de behoefte aan een handreiking die opdrachtgevers en leveranciers laat zien wat je kan doen om samen tot veilige software te komen. Vervolgens is er een werkgroep opgericht en zijn we gaan schrijven. Vooral Marcel Koers, toenmalig CISO van het UWV, heeft hier het schrijfwerk verricht, geholpen door vele andere specialisten.

We hoefden hier natuurlijk niet het wiel uit te vinden want er is al veel ontwikkeld en geschreven. De kunst was om het handzaam en duidelijk bij elkaar te brengen en in een haalbare vorm te gieten. Dat is gelukt door gebruik te maken van volwassenheidsniveaus. Iedereen kan het.

De methode

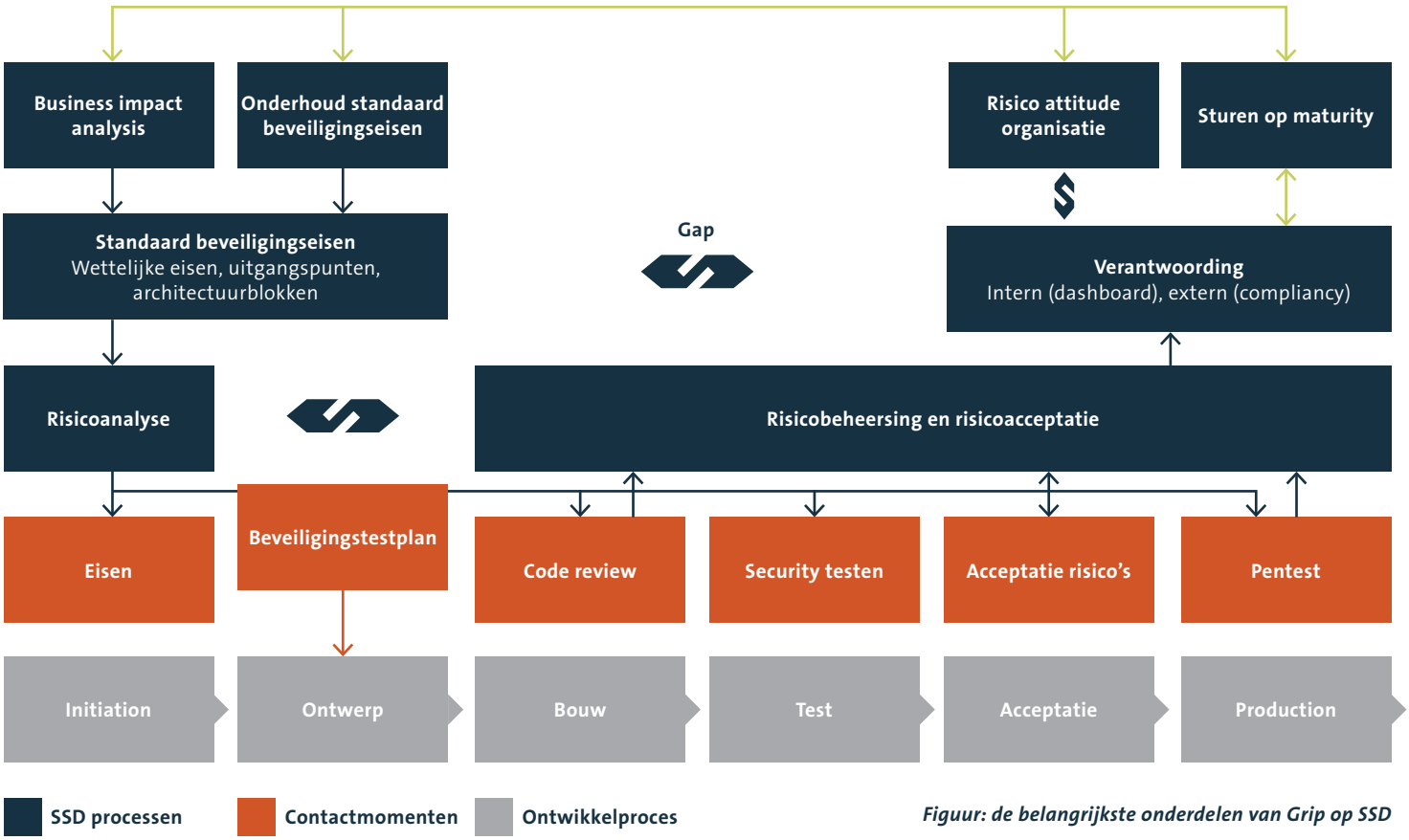
De methode Grip op SSD beschrijft hoe een opdrachtgever grip krijgt op het laten ontwikkelen van goed beveiligde software. Dat kan bij een interne ontwikkelafdeling zijn of bij een externe leverancier. De drie pijlers van de methode zijn 1) standaard beveiligingseisen, 2) contactmomenten en 3) het inrichten van de juiste processen. Deze processen zijn onder meer het bijhouden van risico's, onderhouden van eisen en het laten groeien van de organisatie naar hogere volwassenheidsniveaus. Voor de definitie van de normen is een nieuwe, fundamentele beschrijvingswijze (SIVA) gehanteerd, met zeggingskracht voor managers, ontwikkelaars, testers, auditers en securityspecialisten.

De normen zijn gestoeld op de NCSC-richtlijnen voor (web)applicaties. Per norm wordt de link gelegd naar gerelateerde richtlijnen van NCSC en van OWASP ASVS (Application Security Verification Standard). Ook wordt per onderdeel aangegeven wie verantwoordelijk is: opdrachtgever, bouwer of bijvoorbeeld hostingpartij. Inmiddels heeft IBM de normen laten vertalen naar het Engels.

Welk probleem lost dit op?

Eerder gaf ik al aan dat het slecht gesteld is met de veiligheid van software. We hoeven de krant maar open te slaan om dit bevestigd te zien. Om te illustreren waar het misgaat zal ik een aantal uitspraken uit de praktijk delen en daarbij aangegeven hoe Grip op SSD daarop inspeelt.

Organisatorische inrichting SSD



Figuur: de belangrijkste onderdelen van Grip op SSD

“Wij gaan ervan uit dat een leverancier weet hoe je veilige software maakt”

Op zich is dat een goede positieve instelling. Maar hoe weet de leverancier wat jij veilig genoeg vindt voor de toepassing? Dat zul je moeten afstemmen. Bovendien, als je helemaal niets opschrijft, maar alleen beschrijft wat de gebruiker moet kunnen, dan zal die leverancier zich vooral daarop concentreren als de tijd gaat dringen. Daar kan hij namelijk aan gehouden worden. Grip op SSD beschrijft wat je van tevoren met een leverancier kunt afspreken, hoe je daarover afstemt met “comply or explain” en wanneer je met welke methodes kunt toetsen.

“Ik dacht dat de hostingpartij dat zou regelen”

Deze horen we wel vaker. Wie zou nou de patching van de libraries doen? Grip op SSD maakt expliciet waar de verschillende verantwoordelijkheden en taken liggen.

“We hadden eerlijk gezegd niet verwacht dat die security-eisen getoetst zouden worden”

In de praktijk is er weinig toezicht op het werk van een softwarebouwer. Men is vaak verrast als er een codereview wordt uitgevoerd. Ontwikkelaars willen wel graag veilige software schrijven, maar eisen zijn niet duidelijk genoeg of ontbreken, en als ze er zijn worden ze niet of pas laat getoetst, bijvoorbeeld met een pentest. Een leverancier fixt dan de daarin gevonden lekken en het is klaar.
Typisch gebeurt dat in de drukste periode, namelijk vlak voor de release, dus er is onvoldoende tijd voor structurele

“Ik hoop dat SSD wordt geadopteerd door de gehele overheid en dat men zich hieraan wil committen, een absolute win-win situatie voor zowel bedrijfsleven als overheden.”

Capgemini

verbeteringen. Dat is geen security by design, dat is security after the fact. Grip op SSD beschrijft hoe je duidelijk kunt zijn naar een softwarebouwer en hoe je een ontwerp kunt toetsen en vervolgens tijdens de ontwikkeling ook de afspraken kunt toetsen door middel van codereview.

"O, leidt dat tot reputatieschade?"

Dat is een quote van een ontwikkelaar. In de praktijk blijkt dat softwarebouwers onvoldoende begrijpen wat de gevolgen zijn van bepaalde fouten. Grip op SSD geeft aan dat de resultaten van risicoanalyses worden gecommuniceerd naar alle ontwikkelaars, zodat er meer bewustzijn is.

"Het moet aan de OWASP top 10 voldoen"

Deze top 10 is heel belangrijk in het kweken van bewustwording, maar is ongeschikt als afspraak, want de OWASP is niet specifiek en compleet. Bovendien is de OWASP top 10 een lijst van kwetsbaarheden en niet van eisen. Eén van de OWASP top 10 kwetsbaarheden is "het lekken van gevoelige data". Als opdrachtgever wil je dat inderdaad voorkomen, maar wanneer vind je dat je leverancier hier voldoende aan gedaan heeft? De standaard beveiligingseisen in Grip op SSD zijn hier expliciet over. We zien nu dat bij het toepassen van Grip op SSD de betrokken opdrachtgevers en software-ontwikkelaars beter weten waar ze aan toe zijn en hopelijk horen de bovenstaande uitspraken binnenkort tot het verleden.

"Alles overziend komen we tot de conclusie dat dit document (vanwege het gebruik van SIVA) veel bruikbaarder is dan andere normenkaders die we hebben gezien."

TNO

Grip op Secure Software Development is het resultaat van markt-brede samenwerking tussen specialisten, opdrachtgevers en leveranciers, onder de paraplu van het Centrum voor Informatiebeveiging en Privacybescherming (CIP).
Bekijk ook het onderdeel 'Producten' op www.cip-overheid.nl voor meer informatie.

Over SIG

De Software Improvement Group (SIG) helpt organisaties en technologieleiders hun bedrijfsdoelstellingen te realiseren door de staat en security van hun software fundamenteel te verbeteren. SIG combineert haar eigen tools en benchmarkgegevens met de expertise van haar consultants om organisaties te helpen bij het meten, evalueren en verbeteren van de kwaliteit van hun code – of het nu gaat om het bouwen, kopen of beheren van software.

Als onafhankelijke organisatie heeft SIG de grootste benchmark in de sector met meer dan 36 miljard coderegels verspreid over honderden technologieën. De deskundige consultants van SIG gebruiken deze benchmark om de IT-assets van een organisatie te analyseren op onderhoudbaarheid, schaalbaarheid, betrouwbaarheid, complexiteit, security, privacy en andere bedrijfskritieke factoren. Het SIG-laboratorium is het enige ter wereld dat geaccrediteerd is volgens ISO/IEC 17025 voor de analyse van softwarekwaliteit.

SIG, opgericht in 2000 als een spin-off van de Universiteit van Amsterdam, blijft qua aanpak sterk geworteld in de academische wereld. Het bedrijf werkt internationaal voortdurend samen met universiteiten en onderzoeksinstituten om haar evaluatiemodellen voor softwarekwaliteit en R&D-inspanningen verder te ontwikkelen. SIG heeft hoofdkantoren in Amsterdam en New York en regionale kantoren in Kopenhagen, Antwerpen en Frankfurt. Meer informatie over SIG vindt u op www.softwareimprovementgroup.com.

Fred. Roeskestraat 115
1076 EE Amsterdam
The Netherlands

www.softwareimprovementgroup.com
marketing@softwareimprovementgroup.com