KPMG

De vijf elementen voor DevSecOps die de overheid nodig heeft

Digitale kwetsbaarheden en dreigingen hebben bij veel overheidsorganisaties een omvangrijke digitale transitie in gang gezet. Applicaties worden grootschalig vernieuwd en naar de cloud gebracht. Bovendien wordt steeds meer data gedeeld tussen overheidsorganisaties, bedrijven en de burger. Deze toenemende digitalisering maakt het verbeteren van de cybersecurity bij overheidsorganisaties steeds belangrijker. Dat geldt ook voor de aanschaf, de ontwikkeling en integratie van nieuwe software. Het 'by design' – dus al voordat software wordt ontwikkeld of geïmplementeerd – meenemen van securityvereisten in plaats van deze pas laat in het softwareontwikkelproces te toetsen, is een goede manier om problemen of rework in een latere fase te voorkomen. DevSecOps vertegenwoordigt die paradigmaverschuiving waarbij beveiliging een 'shift left' maakt in het softwareontwikkelproces. Door het omarmen van principes van 'security by design' en 'privacy by design' wordt de security- en privacyimpact al in een vroeg stadium meegenomen.

Ontwikkelen, beheren én beveiligen bij één team

Waar DevOps eerder betekende dat ontwikkeling en beheer werden samengevoegd in één team, is de volgende stap om ook security integraal te betrekken (zie inzet). In het verleden werden ontwikkelde systemen vaak over de schutting gegooid naar het beheerteam, met als resultaat een gebrek aan inzicht en verantwoordelijkheid. Het credo "you build it, you run it" brak met deze scheiding en recentelijk klinkt dus steeds luider de roep om ook security meteen te integreren. Technologische vooruitgang en beschikbare tools maken het overigens veel makkelijker om dat te doen.

Goede security vanaf het begin: veiliger, sneller én goedkoper

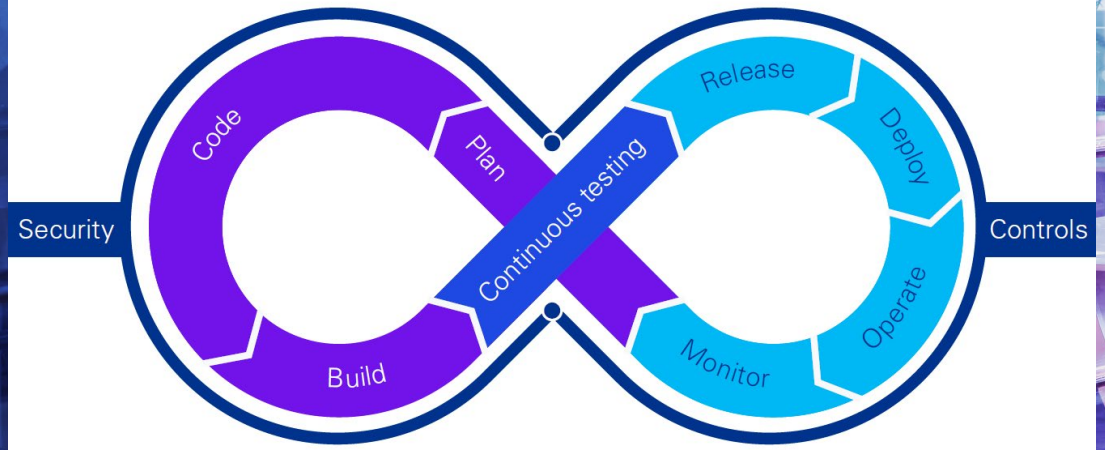
De voordelen van DevSecOps zijn talrijk. Niet alleen worden fouten sneller ontdekt, wat kosten bespaart, maar ook ontstaat er een groter bewustzijn bij ontwikkelaars over het belang van beveiliging. Het vooruitbrengen en actief nadenken over security maken veiligheid toegankelijker en dragen bij aan het opbouwen van snelheid in het ontwikkelproces. In deze context worden maatregelen rondom security en privacy niet langer als een last gezien, maar als een waardevolle troef voor veiligere, efficiëntere en bewustere softwareontwikkeling binnen de overheid.

Recente ontwikkelingen in relatie tot DevSecOps

- Sinds 2023 werkt het National CyberSecurity Center of Excellence (NCCoE) van NIST aan het ontwikkelen en documenteren van een risk-based approach rondom secure DevOps in aansluiting op het Secure Software Development Framework (SSDF). De eerste resultaten worden in 2024 verwacht.
- De handreiking 'Grip op Secure Software Development (SSD) van CIP-overheid is opgezet vanuit het perspectief van een opdrachtgever die regisseert en stuurt op de ontwikkeling van gebruikersvriendelijke en veilige applicaties, zonder in te willen breken in het ontwikkelproces van interne of externe softwareleveranciers. Secure Software Development concretiseert daarmee de eisen en richtlijnen vanuit de BIO. Het whitepaper 'Agile Security Management' geeft handvatten hoe informatiebeveiliging kan worden ingepast in een agile werkwijze.

Van DevOps naar DevSecOps: een evolutionaire stap

DevSecOps is een softwareontwikkelingsfilosofie, waarbij securityprincipes en -controls zo veel als mogelijk worden geïntegreerd en geautomatiseerd in iedere fase van het software-ontwikkelproces. Door vraagstukken rondom beveiliging al mee te nemen in het ontwerp-proces, maar ook door het maximaal automatiseren van het opsporen van kwetsbaarheden tijdens het ontwikkelen van de software, kunnen onvolkomenheden al in een zo vroeg mogelijk stadium worden ontdekt en direct worden opgelost. Daarmee bouwt DevSecOps voort op de beweging rondom DevOps die als zo'n vijftien jaar geleden in gang werd gezet. DevOps beoogt om de werelden van Development (Dev) en Operations (Ops) zoveel mogelijk samen te brengen en deze twee bloedgroepen als één team te laten opereren. Om tegemoet te komen aan de wensen om het sneller en betrouwbaarder releasen van software mogelijk te maken wordt door DevOps-teams vaak ingezet op een hoge mate van het automatiseren van de softwareontwikkelpijplijn.



Niet onbelangrijk is dat de beweging naar het toepassen van DevOps-principes samenviel met twee andere grote verschuivingen: de overstap naar de cloud en de groeiende afhankelijkheid van open sourcetechnologie. Deze ontwikkelingen boden veel kansen in het versnellen van de digitale transformatie, maar ze brengen ook uitdagingen met zich mee als het gaat om het beveiligen van applicaties en de bijbehorende infrastructuur. Omdat DevOps-teams sneller en vaker resultaten leveren, is het voor losstaande securityteams moeilijker om bij te blijven. Het meenemen van security-aspecten als integraal onderdeel in het ontwikkelproces (lees: DevSecOps) is daarom een logische evolutionaire stap als het gaat om moderne softwareontwikkeling. Door meer security-expertise in te brengen in het ontwikkelproces kan de autonomie van het ontwikkelteam verder worden vergroot, terwijl er binnen het team ook maximale aandacht is voor beveiliging.

Vijf tips die de adoptie van DevSecOps stimuleren

Een succesvolle DevSecOps-strategie heeft als doel om gedeeld eigenaarschap te creëren tussen verschillende teams en de verantwoordelijkheid daarvoor niet primair bij een apart team of afdeling onder te brengen. Dit betekent vooral een cultuurverandering, waarbij structurele aanpassingen worden gedaan in de manier van werken en het denken over security. Het is daarom van cruciaal belang om ervoor te zorgen dat deze vraagstukken een integraal onderdeel uitmaken van de 'developer experience'[1] om de voordelen ten volle te kunnen benutten.
Vijf tips:

01 Maak ontwikkelaars bewust van privacy- en securityaspecten

Een belangrijke stap is het verbeteren van de bewustwording rondom privacy- en securityaspecten bij het team dat de oplossing daadwerkelijk realiseert.
Vaak nog worden vraagstukken rondom security- en privacy als losstaande, specialistische expertises gezien waardoor in teams onvoldoende kennis aanwezig is en waardoor weer belangrijke keuzes voor of tijdens de softwareontwikkeling niet worden gemaakt.
Dat betekent vaak dat onnodig rework op een later moment op de loer ligt. Training op het gebied van security en privacy is essentieel en draagt bij aan de noodzakelijke hygiëne. Het investeren in bewustwording van wet- en regelgeving binnen de overheid op dit gebied (zoals de vereisten rondom NIST2, de Baseline Informatiebeveiliging Overheid en de gedefinieerde uitgangspunten rondom Secure Software Development van CIP-Overheid) zijn eveneens een belangrijke stap voorwaarts. Ook het vragen om aanwezigheid van relevante kennis bij de inhuur van externe ontwikkelaars draagt bij aan een betere bewustwording.

02 Integreer security in de bestaande manieren van werken

Voor DevSecOps-teams is het van groot belang om security niet langer meer als iets losstaands te beschouwen, maar als integraal onderdeel van de ontwikkelwerkzaamheden. Het integreren van security in de bestaande manieren van werken is essentieel en vereist het maken van goede afspraken rondom de werkwijze. Het in kaart brengen van iedere stap in de software development lifecycle (SDLC) en het bepalen van de noodzakelijke controls zijn noodzakelijk om toe te werken naar een beheerst proces waarin ook security- en privacyaspecten worden geïntegreerd.
De handreiking 'Grip op Secure Software Development' (SSD) van CIP-overheid biedt concrete handvatten om rekening mee te houden.

1) Developer experience (DevEx) refereert naar hoe moeilijk of makkelijk het is voor een ontwikkelaar (of ontwikkelteam) om essentiële taken in het softwareontwikkelproces uit te kunnen voeren. Een positieve developer experience betekent dat taken relatief eenvoudig uitvoerbaar zijn.

03 Breng automatiseringsopties in kaart en automatiseer maximaal

Doorgaans wordt de manier van werken ondersteund door verschillende automatiseringstools. Een veel gehoorde klacht van ontwikkelteams is de fragmentatie van tooling in het ontwikkelproces. Wanneer security-tooling aan de software-ontwikkelpipeline wordt toegevoegd, bestaat het risico van verdere fragmentatie. Het in kaart brengen van deze tooling, maar ook de uit de tooling voortkomende informatie, kan de ontwikkelaar helpen bij het opleveren van kwalitatief goede en veilige software.

04 Creëer duidelijke verwachtingen rondom softwarekwaliteit en secure coding

DevSecOps zou niet moeten gaan over het introduceren van meer tools, maar over het vaststellen van een duidelijke focus rond verwachtingen en processen voor het effectief gebruik van bestaande tools. Duidelijke communicatie over beleid en secure coding practices zorgt voor een consistente benadering van beveiliging in de hele SDLC. Organisaties moeten veilige coderingsstandaarden creëren en vervolgens kampioenen inschakelen om het beleid duidelijk te communiceren tussen teams. Deze aanpak elimineert dubbelzinnigheid, vergroot het veiligheidsbewustzijn onder ontwikkelaars en bevordert een DevSecOps-cultuur in de hele organisatie.

05 Betrek ontwikkelaars intensief bij het maken van beslissingen rondom security

Om een soepele samenwerking tussen development-teams en security-professionals te garanderen, is het van belang om ontwikkelaars intensief te betrekken bij het opstellen van processen rondom beveiliging en het opstellen van beleidsbeslissingen. Het vragen van feedback aan teams voor het implementeren van een nieuwe tool of het wijzigingen van beleid vergroot de mate van adoptie. Het stellen van vragen over de huidige effectiviteit van het ontwikkelproces, de impact van tools op de workflow en aanbevelingen voor tools of in te zetten practices kunnen nuttige inzichten opleveren en bijdragen aan een cultuur van continue bewustwording en verbetering.

Naarmate ontwikkelteams binnen het DevSecOps-gedachtengoed meer verantwoordelijkheid rondom privacy- en securityaspecten op zich nemen, wordt het verbeteren van hun developer experience van cruciaal belang. Bedrijven en overheden die investeren in het begrijpen en aanpakken van de pijnpunten van DevSecOps-teams zullen daarvan zeker baat hebben. Immers, met ontwikkelaars als ‘first line of defense’ kunnen overheden de voordelen van DevSecOps ten volle benutten.

Hoe wij kunnen helpen?

Bij KPMG kunnen we overheden helpen met het zetten van de volgende stap in de digitale transformatie. Op basis van onze methoden en hulpmiddelen zijn we niet alleen in staat om uw huidige volwassenheidsniveau in kaart te brengen, we kunnen u ook een stap verder helpen in de implementatie. We zijn goed op de hoogte van de voor de overheid geldende wet- en regelgeving en volgen de ontwikkelingen op de voet. Dat geldt ook voor de nieuwe ontwikkelingen op het gebied van DevSecOps. We praten graag verder over alle mogelijkheden.

Contact

Meer informatie?

Bent u benieuwd naar meer details of heeft u andere vragen? Wij gaan graag met u in gesprek. Neem contact op met een van onze experts.

Jos van Brummelen

Senior Manager
Digital Enablement

vanbrummelen.jos@kpmg.nl
T +31 (0)6 46 37 87 55

Deborah Hofland

Partner

hofland.deborah@kpmg.nl
T +31 (0)70 338 24 21

www.kpmg.nl

April 2024