Secure Development Lifecycle (SDLC)

Zekerheid inbouwen tijdens het ontwikkelproces

Zwakheden kunnen op elk moment in het ontwikkelproces onstaan. Naast de fouten in programmatuur en configuratie kunnen deze ook zitten in requirements architectuur en design. Onderzoek heeft aangetoond dat de helft van de security issues al aanwezig is voordat er ook maar 1 regel is geprogrammeerd.

sogeti
Part of Capgemini

Geen verrassingen

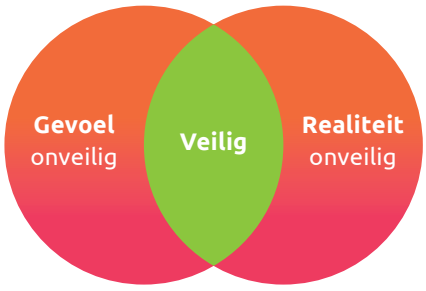
Zowel tijdens het ontwikkelen als tijdens de lifecycle van systemen en applicaties wil je zoveel mogelijk zekerheden inbouwen, of anders gezegd: je wilt achteraf niet voor verrassingen komen te staan. Vaak worden IT-ontwikkelingen toch pas achteraf getest en worden onzekerheden ontdekt op het moment dat men net dacht klaar te zijn. Wat volgt, is een tijdrovend en kostenverhogend proces van extra controles, reviews, terugdraaien en opnieuw bouwen. Daarom ontwikkelde Sogeti een andere zienswijze op Proactive Security Strategy kortwerk PaSS. Binnen PaSS zit het SDLC gedachtegoed ingebakken.

Meer zekerheid, minder fouten

Met een SDLC ben je op het gebied van security niet alleen afhankelijk van de achteraf toegepaste pentest, maar worden verwachtingen en behoeften al tijdens het ontwikkelproces gemanaged. Want hoe eerder iets wordt opgelost, hoe goedkoper en veiliger het is. Daardoor kan er meer zekerheid worden ingebouwd, is er minder kans op fouten, wordt ongewenst gedrag van het systeem tijdig getackeld en kan er sneller gereleast worden.

Gebaseerd op feiten en ratio

Er zijn talloze manieren om veiligheid te omschrijven, maar een van de meest gehoorde is veiligheid is 'een gevoel'. Dit is maar ten dele waar. Slechts het punt waar het gevoel overeenkomt met de werkelijkheid is veilig. Het adopteren van een Secure Development Lifecycle heeft als doel de cirkels van gevoel en realiteit beter te laten overlappen, waardoor beslissingen over informatiebeveiliging gebaseerd worden op feiten en ratio in plaats van gevoel.



Wat is nodig?

Het implementeren van SDLC is een strategische keuze, maar deze keuze kost tijd. Het vereist een mission statement waarin betrouwbaarheid een terugkerend woord is en een management dat dit uitdraagt. Hierdoor ontstaat een cultuur waarin men kritisch kan zijn. Alle participanten in de keten; van producteigenaar tot architect en van ontwerper tot tester, zullen zich bewust moeten zijn van hun rol en invloed op het ontwikkelproces. Dat begint met een collectieve bewustwording; met elkaar een eenduidig beeld hebben van het functioneren van de keten.

Sogeti doet voor, draagt bij of legt uit

Om die bewustwording te sturen, helpt Sogeti bij het in kaart brengen van de behoeften, verwachtingen en eisen. Aan de hand van een nulmeting wordt het huidige niveau inzichtelijk gemaakt. Gezamenlijk bepalen we wat het gewenste niveau in elke stap van de ontwikkelketen. Uitgangspunt daarbij is dat een procesverbetering volgens SDLC 'lean' moet zijn. Alleen daar waar kostenneutrale risicoreductie plaats kan vinden, worden structurele verbeteringen doorgevoerd. Deze zogenaamde secure requirements vormen een leidraad voor verbetering en bieden alle participanten in het ontwikkelproces houvast.

Kortcyclisch nadenken

SDLC is een mindset die uitstekend past bij een agile werkwijze. Elke sprint die in zo'n agile omgeving wordt gemaakt, biedt de kans om kortcyclisch na te denken over beveiliging en veiligheid. Om de brug te slaan tussen uw beveiligingswensen en het eindproduct kijkt Sogeti naar het proces wat áchter de ontwikkeling schuilgaat. Als gerenommeerd IT dienstverlener begrijpt Sogeti hoe ontwikkelprocessen werken. Als uw security partner zorgen wij ervoor dat beveiliging hiervan een integraal onderdeel wordt.

Sogeti traint en begeleidt

Medewerkers van Sogeti draaien embedded mee in uw team. Zij trainen en begeleiden medewerkers in het ontwikkelproces van SDL. Waar nodig valideren zij deze, bijvoorbeeld door het uitvoeren van een Security Assessment. Sogeti-medewerkers hebben een grote passie en ruime praktijkervaring. Door hun betrokkenheid bij de internationale security community bevinden zij zich bovendien op het snijvlak van geldende standaarden en de innovatie. Zij beschikken over toonaangevende certificeringen zoals CISSP, CISM en OSCP en nemen onder andere deel in de NEN-normcommissie.

Meer weten? Bel of mail ons op security@sogeti.nl

Over Sogeti

Sogeti is een toonaangevende leverancier van technologie en engineering diensten. Sogeti levert oplossingen die digitale transformatie mogelijk maken en biedt specialistische kennis in Cloud, Security, Digital Manufacturing, Digital Assurance& testen en opkomende technologieën. Sogeti combineert flexibiliteit en snelheid van implementatie met sterke technologiepartners, innovatieve methodologieën en haar wereldwijde leveringsmodel, Rightshore®. Sogeti brengt meer dan 25.000 professionals samen in 15 landen, gevestigd in meer dan 100 vestigingen in Europa, de VS en India. Sogeti is een 100% dochteronderneming van Capgemini SE, genoteerd aan de Parijse beurs.

Leer meer over ons op

www.sogeti.com

Meer weten? Neem contact op met:
Pieter Lacroix
Tel +31 (0)88 880 66 00
pieter.lacroix@sogeti.com

Sogeti Nederland B.V. | Lange Dreef 17 | 4131 NJ | Vianen
Tel +31 (0)88 880 66 00
sogeti.nl/soc