Application Security

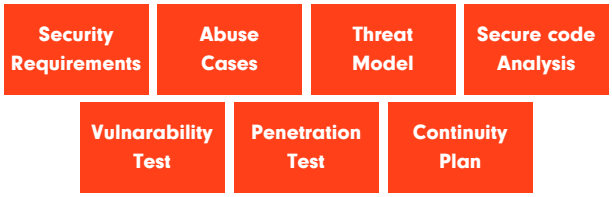
Hoe veilig zijn we eigenlijk?

Door de continue druk van steeds sneller nieuwe producten te lanceren, wordt informatiebeveiliging vaak als niet-functionele eis en daardoor ondergeschikt beschouwd. Als organisatie wil je zeker stellen dat de veiligheid van jouw klant is geborgd en dat kans op fraude minimaal is. Zo stelde een grote speler in de bancaire sector aan Sogeti de vraag: "Hoe veilig zijn wij eigenlijk?"Als reactie op deze vraag voerde Sogeti een penetratietest uit.
Uit de test kwamen verschillende kwetsbaarheden en risico's naar voren, die herleid werden naar het ontwikkel- en ontwerpproces. De klant kreeg inzicht dat er onvoldoende aandacht is besteed aan de veiligheid van hun applicaties,waardoor de kwetsbaarheden zijn ontstaan.

Application Security is méér dan een test.
Application Security is het samenspel tussen mensen, processen en techniek binnen een organisatie. Sogeti beheerst zowel de organisatorische - als technische aspecten en is ervan overtuigd dat de juiste beslissingen op het gebied van security gebaseerd zijn op feiten en kennis in plaats van gevoel en emotie. Application Security is niet het nemen van zo veel mogelijk maatregelen, maar juist het bewust investeren daar waar nodig. Zodat een security test de veiligheid bevestigt en je niet in een later stadium wordt verrast.

Veiligheid leidt tot een betere afstemming van de activiteiten.
In iedere fase van de lifecycle van een applicatie ontstaan kwetsbaarheden, risico's en bedreigingen. Elke deliverable brengt namelijk zijn eigen type kwetsbaarheid met zich mee. Om veiligheid in de hele lifecycle te garanderen moet security in elke fase worden geïmplementeerd. Sogeti noemt dit een Secure Development Lifecycle (SDLC)

Hierbij is Application Security niet langer exclusief voor de specialist, maar een onderdeel van ieders werkzaamheden. Dit betekent niet dat er nieuwe activiteiten worden toegevoegd. Het streven is immers om bestaande werkzaamheden uit te voeren met een hoger bewustzijn van veiligheid.



Om een SDLC te implementeren zijn er verschillende deelactiviteiten te onderscheiden:

Security Requirements
Door middel van een risico-inventarisatie worden secured requirements opgesteld.

Abuse Cases
Naast Use-cases worden negatieve varianten van use-cases uitgewerkt. Wat wil je echt niet, is de vraag die je steeds moet stellen.

Threat Model
Een geprioriseerd overzicht van alle gedefinieerde bedreigen wordt gemaakt op basis van architectuur en ontwerp.

Static Code Analysis
Tijdens een security code analyse worden afwijkingen en kwetsbaarheden in de broncode gedetecteerd.

Vulnerability test
Een 360 graden onderzoek naar bestaande technische kwetsbaarheden, ontwerp- en logica fouten in software, infrastructuur en organisatie.

Penetration test
Tijdens een penetratietest worden kwetsbaarheden geëxploiteerd om een vooraf gedefinieerd risico te bevestigen.

Continuity plan
Ga ervan uit dat een risico realiteit wordt, dan kan je vooraf een plan maken om businessprocessen te laten continueren.

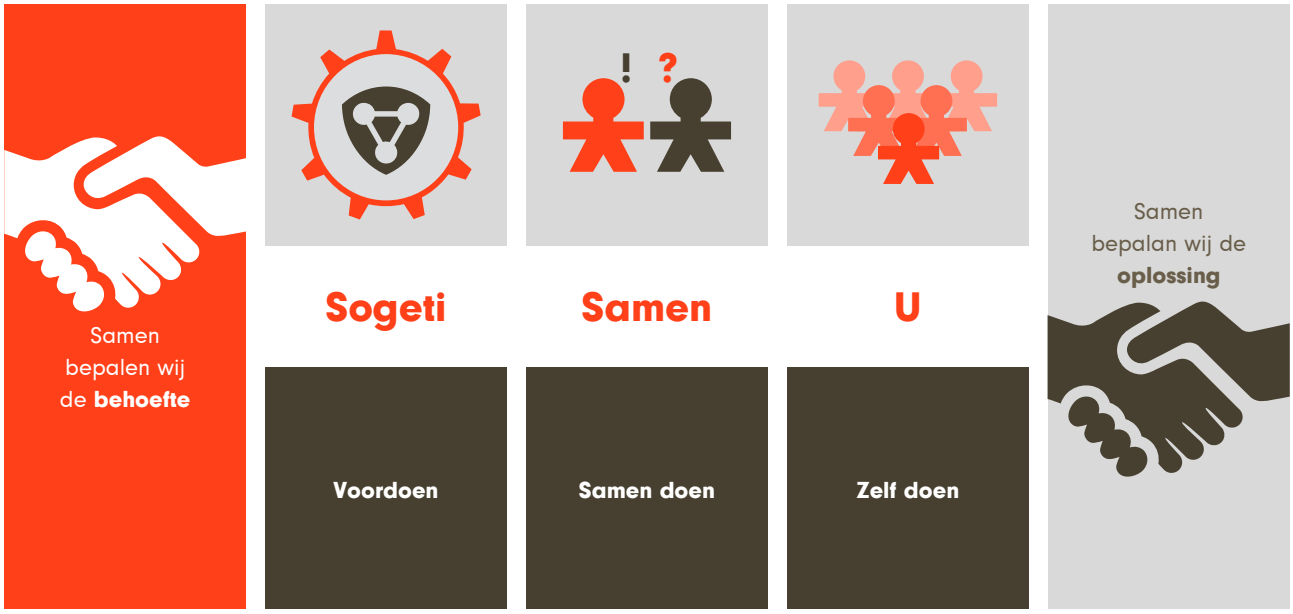
De volgende stap: Groei en volwassenheid.
Het aan de slag gaan met Application Security is een strategische keuze. Sogeti helpt u bij het in kaart brengen van behoeften en doet dit aan de hand van maturity-modellen. Hierin specificeert u zelf wat de gewenste niveau zijn in elke stap van de ontwikkelketen. Een procesverbetering zoals de SDLC moet volgens Sogeti LEAN zijn; alleen daar waar kostenneutrale risicoreductie plaatsvindt, worden structurele verbeteringen doorgevoerd. Afhankelijk van de beschikbare middelen en kennis kan de klant kiezen uit drie vormen van dienstverlening:

- Voordoen: Sogeti neemt de volledige implementatie voor haar rekening zodat u zich kan blijven richten op haar kernactiviteiten;
- Samen doen: Sogeti werkt samen met u aan de implementatie;
- Zelf doen: U verzorgt zelf de implementatie waarbij Sogeti training of advies levert.

Het resultaat.
U heeft controle over uw IT. U investeert gericht. U neemt berekende risico's. Door te investeren op de juiste plaats in de organisatie, software en infrastructuur, bent u veilig. Daarnaast helpt Application Security de kwaliteit van de informatiesystemen verbeteren en kunt u veilig en snel nieuwe producten op de markt brengen. Dit betekent: 'In één keer goed!'

Door Application Security te implementeren kunt u op elk moment antwoord geven op de vraag "Hoe veilig zijn we eigenlijk?"

Conclusie
Wilt u controle hebben over uw IT-veiligheid en zonder aarzelen de vraag "hoe veilig zijn we eigenlijk", kunnen beantwoorden, neem dan contact op met Rogier van Agt.



Sogeti Nederland B.V.
Sogeti is een multi-IT specialist actief in applicatiebeheer, management van infrastructuren en (High-Tech) engineering. De oplossingen van Sogeti voor mobile, security, de cloud en business intelligence dragen bij aan het realiseren van de strategische doelstellingen van haar klanten in de grootzakelijke markt. Op het gebied van softwaretesten is Sogeti marktleider, zowel wereldwijd als in Nederland. Passie voor het vakmanschap zit in de genen van de 3000 Sogetisten werkzaam (dicht) bij de klant. Sogeti Nederland B.V. maakt deel uit van de wereldwijde Sogeti-groep met zo'n 20.000 IT- professionals in vijftien landen met meer dan honderd vestigingen in Europa, de VS en India.
Meer informatie is beschikbaar op **www.sogeti.nl**

Sogeti Nederland B.V.
Lange Dreef 17
Postbus 76
4130 EB Vianen

Tel +31 (0)88 660 66 00
Fax +31 (0)88 660 67 00
www.sogeti.nl/security

SOGETI