‘GAME OVER’ voor cybercriminelen

Spelenderwijs werken aan applicatie-security

Eén van de belangrijkste uitdagingen voor financiële instellingen is cybersecurity. Bijvoorbeeld voor een bank met vele miljoenen rekeninghouders is de veiligheid van systemen cruciaal.

Uitdagingen voor de klant

Datalekken en andere onwenselijke gebeurtenissen moeten voorkomen worden. Tevens is er veel druk om aan regelgeving te voldoen, bijvoorbeeld op het gebied van GDPR.

De weerbaarheid van de bank kan alleen gewaarborgd worden als de technische IT omgeving aan hoge standaarden voldoet. Dit betekent dat veel engineers zo goed mogelijk hun taken moeten uitvoeren op het gebied van cybersecurity. De manier waarop dit gebeurt, wordt gestuurd vanuit security officers en policies. Samen met de teams die verantwoordelijk zijn voor het bouwen en onderhouden van applicaties worden security gerelateerde activiteiten op het gewenste niveau uitgevoerd. Hier ontstaat een interessant spanningsveld.

Helaas blijkt dat het uitvoeren van security gerelateerde werkzaamheden nog wel eens een sluitpost is. Werken aan ‘echte’ functionaliteit gaat dan voor en deadlines zorgen ervoor dat security activiteiten worden doorgeschoven. Een deel van de ontwikkelaars vindt security geen leuk aspect van het werk. Als gevolg hiervan steken security officers, maar ook development managers, erg veel tijd in het sturen van hun teams. Procedures, tools en trainingen worden niet altijd op waarde geschat door DevOps teams. Security volwassenheid is daardoor niet altijd op het gewenste niveau.

Ons antwoord

CGI heeft hier de afgelopen jaren in geïnvesteerd en samen met de CGI Game Factory, de CGI Security Practice en de klant de Security Game gebouwd.

CGI Game Factory

De CGI Game Factory heeft een bewezen track-record in het creëren van leuke en effectieve serious game-ervaringen voor klanten in verschillende sectoren zoals logistiek, onderwijs en de financiële sector. Door het implementeren van serious games en gamification bereiken onze klanten positieve gedragsverandering bij medewerkers, inzicht in complexe processen en kunnen ze medewerkers efficiënt trainen door het inzetten van (Augmented Reality/Virtual Reality) simulaties.

De kracht van deze videogame is dat er elke sprint ongeveer 15 minuten wordt gespeeld. Engineers in een DevOps team spelen het spel gezamenlijk in een vergaderruimte of online. Tijdens het spel wordt een verdediging gebouwd die bestand is tegen dreigende vijanden. Het doel is om met zo min mogelijk uitgaven een verdediging te creëren, zodanig dat data en geld beschermd zijn. Een belangrijk aspect van de game is dat teams een krachtiger verdediging kunnen neerzetten en dus een grotere kans hebben hoog in de teamcompetitie te eindigen, door tijdens hun sprint een aantal gedefinieerde security activiteiten uit te voeren. Dit zijn activiteiten die normaliter wat achterblijven qua uitvoering, maar die nu door toepassing van gamification met meer motivatie worden opgepakt. Dit zijn bijvoorbeeld activiteiten op het gebied van security tests of secure coding.

Voordelen voor de klant

Door het definiëren van deze acties en een hogere motivatie voor teams om de acties uit te voeren, bereiken teams sneller een hoger volwassenheidsniveau. De klant kan de acties zelf definiëren en als een bepaald resultaat is behaald, kan een volgende actie in de game worden opgenomen. Een uitgebreide rapportage geeft de mogelijkheid om per team, maar ook op een geaggregeerd niveau, de voortgang van de teams te analyseren. Dit is op het gebied van de acties die voor volwassenheid gaan zorgen, maar ook op het gebied van de security vragen. Indien gezien wordt dat teams moeite hebben met een bepaald onderwerp, dan kan hier door middel van een training extra aandacht aan worden gegeven.

Als onderdeel van de game beantwoordt elk team 6 security vragen per sprint. Deze vragen zijn van een dusdanig niveau dat teams er in hun dagelijkse werk iets aan hebben. Dit is inclusief codevragen, waar teams gevraagd wordt kwetsbaarheden te zoeken. Een klant kan, indien gewenst, zelf specifieke vragen toevoegen.

Een groot aantal teams heeft inmiddels kennis gemaakt met de game en het is zichtbaar dat de ontwikkelaars het leuker vinden om met security bezig te zijn. Ze doen meer kennis op en tegelijkertijd neemt de security volwassenheid van de teams toe.

Waarom CGI?

CGI combineert innovatie met kennis en ervaring van Serious Gaming en Gamification. En CGI is met gespecialiseerde teams georganiseerd rondom klanten. Daardoor weten teams goed wat er speelt bij de klant en kunnen teams zich volledig concentreren op onze dienstverlening aan de klant. Dit is de reden dat de klant voor CGI heeft gekozen.

‘GAME OVER’ voor cybercriminelen.

Over CGI

CGI, opgericht in 1976, behoort tot de grootste IT en business consultancy bedrijven ter wereld. Wij werken op basis van inzichten en resultaat om het rendement van uw investeringen te maximaliseren. In 17 bedrijfstakken op 400 locaties wereldwijd bieden we uitgebreide, schaalbare en duurzame IT- en business consultancy diensten die wereldwijd beschikbaar worden gesteld en lokaal worden geleverd.

Voor meer informatie

Bezoek cginederland.com
Mail ons via info.nl@cgi.com