Security testing

Van risico naar controle

Secure Development Lifecycle

Website | Mobile | ERP (SAP) | Infrastructure | Maatwerk

Penetratietest

Vulnerability-test (Black/Grey/White)

Manual verification

Automated test

Een bekende vermogensbeheerder ontwikkelt een omgeving waarin klanten zelf hun beleggingen kunnen samenstellen en beheren. Voor deze financiële organisatie is de online dienstverlening een belangrijke groeimarkt en daarom begrijpt ze als geen ander dat online systemen veilig en betrouwbaar moeten zijn. Betrouwbaarheid is het sleutelwoord om ervoor te zorgen dat haar klanten de omgeving ook echt gaan gebruiken. Imagoschade ondermijnt de acceptatie van het systeem bij de eindgebruiker, wat een groot risico vormt. Door de Sogeti penetratietest en vulnerability-test te combineren, stellen we deze klant in staat aan te tonen dat de dienstverlening veilig is. Security is daarmee een enabler van de business, omdat hun relaties zich op basis van aantoonbare feiten veilig voelen bij hun online diensten.

Ken uw kwetsbaarheden

Uw IT-omgeving wordt steeds complexer. Ontwikkelingen als Bring Your Own Device, Mobile, Cloud en Big Data bieden kansen en hebben tegelijkertijd een grote impact op uw strategie. En daardoor ook op uw security. Voldoet u aan alle normen op het gebied van compliancy? Is uw organisatie in staat om op tijd en adequaat te reageren op steeds weer nieuwe security-risico's, of deze zelfs een stap voor te blijven? Het is zaak risico's in een zo vroeg mogelijk stadium in kaart te brengen om vervolgens tijdige en gerichte maatregelen te kunnen treffen. Met security testing geven we u inzicht in uw kwetsbaarheden en risico's. We helpen uw business aan een betrouwbare, aantoonbaar veilige ICT, zodat u gerust zaken kunt doen.

Onze oplossingen en diensten

Onze testing services zijn gebaseerd op de Secure Development Lifecycle, een complete aanpak met oplossingen die gericht zijn op het identificeren, verminderen en voorkomen van security-risico's en waarmee we onderzoeken hoe veilig uw ICT-diensten zijn. Op basis van uw specifieke security-behoefte kunnen we delen of combinaties van onze diensten inzetten. Door middel van diverse security-tests krijgt u inzicht in hoe toereikend uw beveiligingsmaatregelen zijn en tonen we zwakheden aan. De kritische invloed van het betreffende systeem op uw business is bepalend voor de zwaarte van de test.
Wij testen onder andere websites, mobile apps, standaard software zoals SAP, uw infrastructuur en/of maatwerkapplicaties. We gebruiken verschillende soorten tests om de security-risico's te identificeren.

Penetratietest

Bij een penetratietest geeft u ons een gerichte opdracht. Bijvoorbeeld: 'Leg deze website plat.' Hiermee valt aan te tonen of de kwetsbaarheden uit de vulnerability-test tot onacceptabele risico's leiden. Denk hierbij aan het benaderen en aanpassen van gevoelige informatie of het onbereikbaar maken van een systeem.

Vulnerability-test

De vulnerability-test voeren we uit op uw operationele applicaties, software en/of infrastructuur. Maar we kijken ook in een vroeg stadium naar mogelijke ontwerpfouten in de documentatie. Binnen een vooraf gestelde 'time box' en gebaseerd op een gestructureerde en bewezen methodiek voeren we een handmatige test uit en brengen zo veel mogelijk zwakheden in kaart.

Onze boxbenadering

Een vulnerability-test kunnen we op verschillende manieren uitvoeren:

Black box - We behandelen de sofware als een black box: zonder vooraf opgeleverde informatie.
Grey box - Zoals bij een black box maar dan vooraf voorzien van systeemdocumentatie.
White box - Zoals bij een grey box maar dan vooraf voorzien van de broncode.

Bugs en flaws
Bij een penetratie- of vulnerability-test zoeken we naar bugs – security-fouten in software of systemen – en flaws – ontwerpfouten in een applicatie/website/systeem die ongewenste functionaliteiten bieden aan hackers bijvoorbeeld. We onderscheiden ons hiermee van standaard geautomatiseerde tests. Door op een andere manier naar processen en functionaliteit te kijken, hebben we bij diverse klanten kritische flaws ontdekt, waarna zij tijdig actie konden ondernemen om schade te voorkomen.

Automated test
Bij een automated test gebruikt de Security Consultant een combinatie van toolkits om de security-test uit te voeren en bekende security-bugs in kaart te brengen. De resultaten van de test worden één op één aan de opdrachtgever beschikbaar gesteld.

Manual verification
Bij de manual verification beoordelen onze security experts nauwkeurig de ongefilterde bevindingen uit de automated test en halen wij de, voor u relevante, bevindingen eruit.

Overige mogelijkheden
Wilt u security-tests uitvoeren, maar liever onder uw eigen regie? Breid uw security-team dan tijdelijk uit met onze experts.

Sogeti biedt op dit gebied ook trainingen aan, zoals een gerichte security-training voor ontwikkelaars (.NET, Java) en technische awareness-trainingen die ontwikkelaars leren denken als een hacker.

Wanneer u uw code op bugs en flaws wil laten controleren, biedt Sogeti Security u Secure code reviews aan. Hiermee haalt u de security-gerelateerde fouten uit uw software, voordat deze live gaat.

Heeft u regelmatig nieuwe releases en verandert uw ICT-omgeving snel? Of wilt u gewoon een vinger aan de pols houden in de bestaande beheeromgeving? Elke dag worden nieuwe kwetsbaarheden gevonden in software, frameworks, servers en applicaties. Op basis van een partnership voeren we onze periodieke security-tests voor u uit en blijft u continu in controle.

Wist u dat
Sogeti sponsor is van OWASP? Onze medewerkers zijn CISSP- en OSCP-gecertificeerd en we voeren projecten uit met PRINCE2.

De volgende stap
De uitkomsten van de security-tests plaatsen we in de context van uw organisatie en zo bepalen we samen met u de business-impact van de bevindingen. Pas als de impact duidelijk is, kan er een zinvolle investering voor een verbeterslag gemaakt worden.
Als eindresultaat van iedere test leveren we u een eindrapport waarin we de bevindingen hebben voorzien van de passende oplossing. Daarmee heeft u concreet inzicht in de prioriteit en de kosten voor verbeteringen, een onafhankelijk advies ten behoeve van auditors en kunt u gerichte keuzes maken om uw concurrenten en hackers voor te blijven.
Sogeti Security testing biedt u op deze manier een helder en concreet inzicht in mogelijke oplossingen voor uw security-risico's, zodat u de stap kunt nemen van risico naar controle.

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
info-is@sogeti.nl
www.sogeti.nl/infrastructuur

SOGETI