Security testing
Omdat elk IT systeem belangrijk is

Security testing

U bent gebaat bij een veilig netwerk en beveiligde applicaties. Wij maken met een aantal diensten inzichtelijk hoe we uw security kunnen optimaliseren. SQA levert een op maat gemaakte oplossing voor uw ICT security behoefte

1. Penetration testing

Een Penetration-test (Pen-test) is een onderzoek waarbij wordt aangetoond of systeem kwetsbaar is voor aanvallen en wat daarvan de mogelijke impact is. Dit is een tijdsgebonden onderzoek waarbij de security specialist met een hacker mindset alle mogelijke middelen en beschikbare informatie gebruikt om het systeem te benaderen, binnen te dringen en waardevolle informatie te vergaren.

Verifieer beveiliging normen en standaarden

Omdat een Pen-test zich voornamelijk richt op het binnendringen van systemen is het belangrijk vooraf goed te bepalen of dit het te bereiken doel is. Wanneer u een volledig beeld wilt krijgen van alle mogelijk te misbruiken kwetsbaarheden in uw systemen, is een vulnerability assessment een meer passende aanpak.

2. Vulnerability testing

Applicaties en netwerken zijn net na het uitvoeren van updates kwetsbaar, omdat bedrijven niet de middelen hebben om iedere nieuwe release in elk project volledig te (laten) controleren. Tot het moment dat controle plaatsvindt, is uw systeem kwetsbaar. U kunt dit risico verkleinen door de systemen periodiek te (laten) scannen.

Beperk het risico van cyber-aanvallen

Een automatische periodieke scan als aanvulling op de handmatige test, detecteert kwetsbaarheden die uw systemen gevoelig maken voor virussen en andere malware. Ook kan het voorkomen dat uw systemen patches missen en bugs in software dus niet hersteld worden. Een security specialist van SQA valideert de resultaten van een automatische scan handmatig om false positives eruit te filteren. Als we kwetsbaarheden aantreffen, rapporteren we deze direct en bieden tevens een advies welke maatregelen te treffen.

3. Compliance Audits

Door middel van compliance audits toetsen wij uw applicaties en infrastructuur aan een bepaalde normenset. Denk hierbij bijvoorbeeld aan Payment Card Industry (PCI) compliance. Een ander voorbeeld van een bekend normenkader is: Open Web Application Security Project (OWASP) ten behoeve van webapplicaties.

Voldoen aan wet- en regelgeving

De compliance audits voeren we uit in combinatie met Vulnerability Testing en Detailed Security Assessment. Dit geeft u direct een compleet overzicht van de eventuele kwetsbaarheden die kunnen resulteren in niet-compliant zijn.

Uiteraard bespreken wij de resultaten met u en kunnen wij u adviseren over eventuele reparaties voor de geconstateerde kwetsbaarheden.

Wij leveren een op maat gemaakte oplossing voor uw ICT security behoefte

4. Infrastructuur Testing

Gezien het belang van uw infrastructuur, nemen wij deze standaard mee in onze kwetsbaarhedenonderzoeken. Er kunnen echter redenen zijn om onderdelen hier buiten te laten. Welke systemen onderdeel moeten zijn van het onderzoek, spreken wij van tevoren goed met u af.

Voorkom virus aanvallen

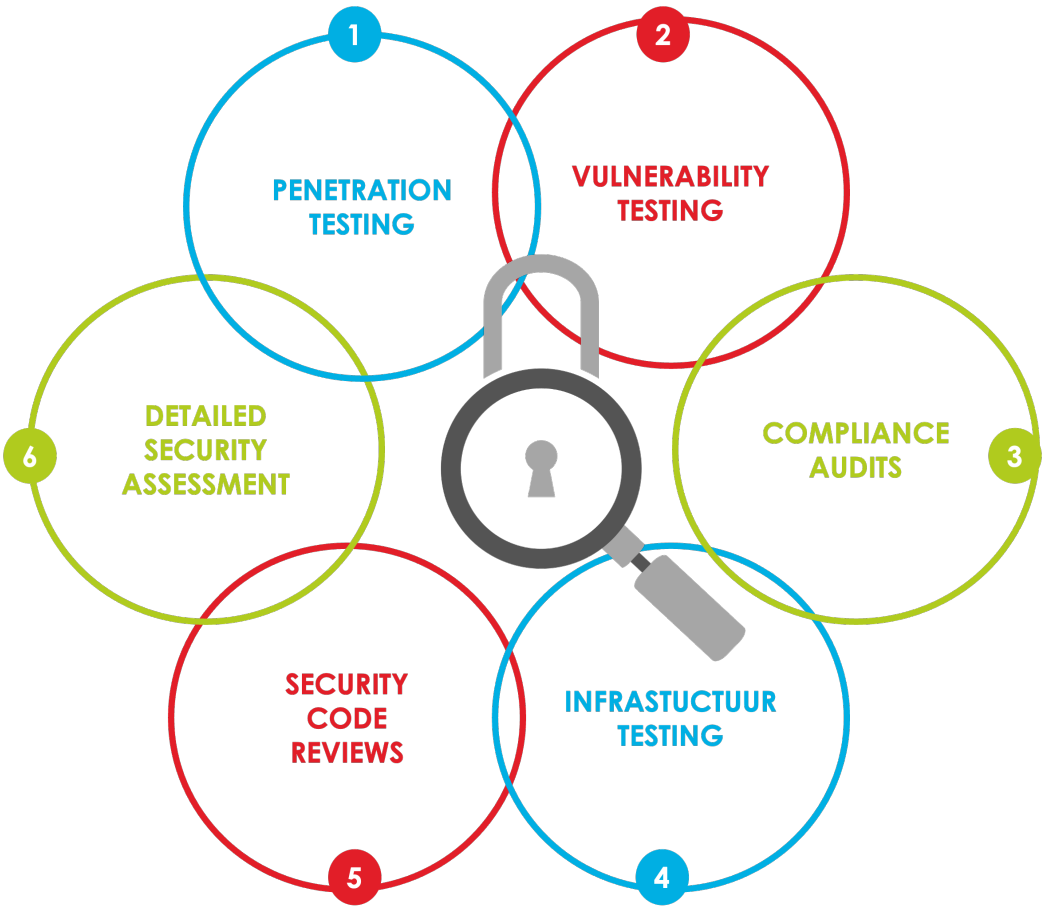
Niet alleen applicaties, ook alle servers en overige infrastructuur waar u gebruik van maakt, spelen een rol in de veiligheid van een omgeving. Daarom onderzoeken wij ook deze systemen volledig op mogelijke kwetsbaarheden. Dit doen wij volgens een vooraf gedefinieerde methode zodat we op een gestructureerde en reproduceerbare wijze een volledig beeld kunnen geven van de veiligheid van de systemen die binnen de scope van de test vallen. Het onderzoek wordt zodanig uitgevoerd, dat het niet (extreem) belastend is voor uw servers en infrastructuur. Dat wil zeggen dat wij kwetsbaarheden identificeren en verifiëren terwijl uw medewerkers gewoon doorwerken. Hun systemen zullen qua performance niet negatief beïnvloed worden. In het geval dat systemen onverwacht reageren op onze invoer, wordt de test onderbroken en nemen wij de vooraf afgestemde acties. Daarnaast zullen wij u adviseren welke maatregelen u kunt treffen om deze kwetsbaarheid te herstellen.

5. Security Code Reviews

Het beschermen van de vertrouwelijkheid van gegevens en het borgen van de beschikbaarheid van uw webapplicatie(s) begint in de basis bij veilig ontwikkelen. Het is verstandig om al vroeg in dit proces aandacht te hebben voor (code) security. Wij kunnen u hiermee helpen door het uitvoeren van code reviews in verschillende stadia van het project.

Veiligheid vanuit de broncode

Een code review is een algemene controle van de broncode waarbij de security specialist gericht zoekt naar kwetsbaarheden binnen de onderdelen die potentieel zwakke plekken bevatten. De bevindingen koppelen we direct terug aan de ontwikkelaars. Ook leggen wij uit hoe eventuele kwetsbaarheden opgelost kunnen worden en dragen wij verbeterpunten aan. Het resultaat van deze aanpak is dat de betrokken ontwikkelaars meer inzicht krijgen in de veiligheid van de systemen en dit kunnen gebruiken in het volledige project. Door security vanaf het begin voldoende te integreren in het proces voorkomt u veel problemen. De kans dat er veel kwetsbaarheden worden gevonden tijdens een handmatig onderzoek (dat vaak aan het eind van het proces uitgevoerd wordt) is aanzienlijk kleiner. Ook lopen releases minder vertraging op. Het uitvoeren van code reviews komt dus niet alleen de veiligheid ten goede, maar ook de voortgang van het project.



6. Detailed Security Assessment

Om uw systemen, applicaties en infrastructuur naar behoren te screenen tegen hackers en andere kwaadwillenden, is het van belang om deze zo volledig mogelijk te onderzoeken op kwetsbaarheden. Een efficiënte methode hiervoor is een detailed security assessment op basis van (vooraf gedefinieerde) checklists. Hiermee geven we op een gestructureerde en reproduceerbare wijze een volledig beeld van de veiligheid van alle gebruikte systemen.

Dit onderzoek kan op verschillende niveaus plaatsvinden, afhankelijk van de scope en risicoanalyse die wij samen met u bepalen. U kunt kiezen voor een aanpak waarbij we voornamelijk controleren op veel voorkomende kwetsbaarheden die eenvoudig misbruikt kunnen worden en een grote impact hebben. Of u kiest voor een uitgebreider onderzoek waarin we ook zoeken naar gecompliceerde kwetsbaarheden die alleen kunnen worden misbruikt door een cybercrimineel met meer motivatie en kennis. Een belangrijk onderdeel van een dergelijk uitgebreid onderzoek is dat tevens defence in depth-items geïdentificeerd worden. Dit zijn maatregelen die u kunt treffen om te zorgen voor een hoger niveau van beveiliging.

Een detailed security assessment (DSA) is anders dan een Pen-test, omdat laatstgenoemde vaak wordt uitgevoerd met als enige doel aan te tonen dat de beveiliging te doorbreken is. Met onze aanpak worden zoveel mogelijk kwetsbaarheden geïdentificeerd die een aanvaller zou kunnen gebruiken voor een (gerichte) aanval. Het DSA kan afgestemd worden op richtlijnen van een audit of om aan bepaalde normen te voldoen, zoals bijvoorbeeld OWASP, NCSC of DigiD.

sqa
TEST US

SQA levert een op maat gemaakte oplossing voor uw ICT security behoefte

Wij geven inzicht in kwetsbaarheden en beveiligingsrisico's. Met behulp van onze diensten en oplossingen kunnen we bedreigingen in een vroeg stadium detecteren nog voordat ze schade kunnen aanrichten. Hierdoor zijn onze klanten weerbaar tegen digitale dreigingen en daarmee voorbereid op de toekomst.

www.sqacaribbean.com