Deloitte.

Risk Services
2014

Hacking as a Service
Kwetsbaarheden veranderen constant, ontdek ze voordat anderen het doen

Maakt u zich zorgen over de beveiliging van uw online presence? Elke change vraagt om een nieuwe hack, daarom hebben wij de oplossing die ervoor zorgt dat u met een gerust hart online zaken kunt doen, namelijk “Hacking as a Service”

Uw uitdaging

Aanvallen op websites en online applicaties zijn aan de orde van de dag en in veel gevallen lekken kostbare bedrijfsgegevens weg. Een van de manieren waarop een organisatie zich hiertegen kan wapenen is het (laten) uitvoeren van security scans. Veel organisaties voeren dit soort security scans echter maar één keer per jaar uit, terwijl cybercriminelen continu nieuwe manieren verzinnen om een organisatie binnen te dringen. Bovendien is de online presence van de meeste organisaties constant in beweging door allerlei nieuwe initiatieven en aanpassingen in bestaande infrastructuur en applicaties. Daarnaast wordt er door wet- en regelgeving steeds meer van uw organisatie geëist.

Onze oplossing

Deloitte heeft een dienstverlening ontwikkeld die ervoor zorgt dat de online presence van een organisatie (infrastructuur en applicaties die via het Internet benaderd kunnen worden) periodiek wordt getest op beveiliging en die direct inzicht geeft in aanwezige kwetsbaarheden. U kunt bij ons een abonnement afsluiten voor deze “Hacking as a Service” dienstverlening, zodat u optimaal gebruik kunt maken van de voordelen die het Internet biedt, terwijl uw actueel inzicht heeft in uw online kwetsbaarheden.

Kenmerken van Deloitte’s Hacking as a Service zijn:

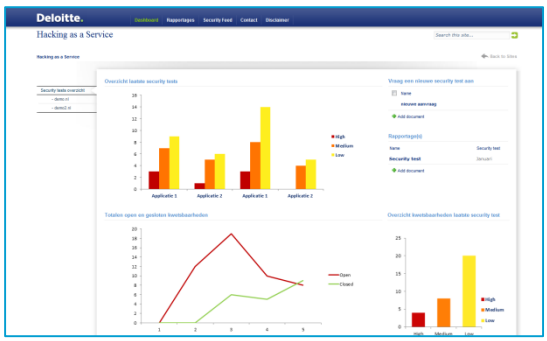
- Op periodieke basis worden de infrastructuur en applicaties getest, de organisatie is niet afhankelijk van één testmoment;
- Continu inzicht in testresultaten door het gebruik van ons Security Dashboard. Uitgebreide rapportage mogelijkheden per periode, per systeem en inzicht in trends die voor meerdere interne en externe doelgroepen kunnen worden gebruikt;
- Bij het verschijnen van nieuwe kwetsbaarheden in software producten die worden gebruikt binnen de online omgeving van uw organisatie bestaat de mogelijkheid direct te testen of een nieuwe kwetsbaarheid zich voordoet;
- Een jaarrapportage met daarin een analyse van de testresultaten van het afgelopen jaar inclusief trends;
- De combinatie van de inzet van tooling en de ervaring van onze professionals zorgt voor een extra toegevoegde waarde: ons team denkt zoals hackers denken en kan technische risico’s vertalen in bedrijfsrisico’s;
- Hacking as a Service kan u helpen met het voldoen aan wet- en regelgeving, zoals richtsnoeren van CBP en DigiD;
- Lage en voorspelbare maandelijkse kosten in vergelijking met eenmalige en ad-hoc testen.

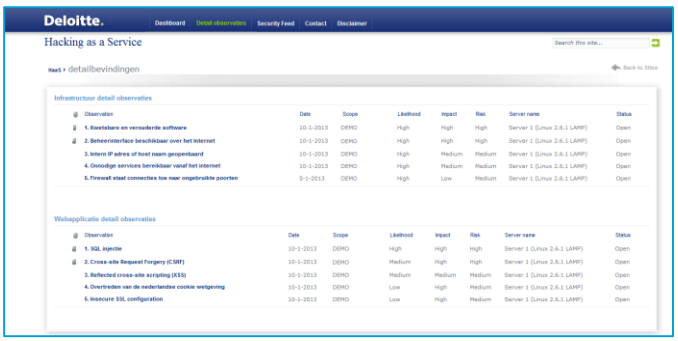
Al deze punten geven u de handvatten om snel te acteren en een verbeterd inzicht in de beveiliging van uw online presence.

Brons	Zilver	Goud
Periodieke security test van Internet-facing infrastructuur componenten op onveilige software en services en aanwezigheid van nieuwe systemen. Deze test simuleert een aanval door een kwaadwillende op de infrastructuur die uw online applicaties ondersteunt.	Idem als Brons. Daarnaast security test van webapplicaties op bekende zwakheden, zoals SQL injection en Cross-Site Scripting (XSS). Deze test simuleert een aanval door een kwaadwillende op uw webapplicaties).	Idem als Zilver. Daarnaast diepgaande security tests van webapplicaties, specifiek op “privilege escalatie” (het ongeautoriseerd toegang krijgen tot informatie of functies als gewone gebruiker). Deze test simuleert een aanval door een kwaadwillende die zich reeds toegang heeft verschaft tot uw online applicaties.

Hacking as a Service	Brons	Zilver	Goud
Kwetsbaarheden rapportage			
• Onveilige software (o.a. verouderde versies van software)	●	●	●
• Onbekende systemen en service	●	●	●
• Onveilige services (o.a. onveilige beheerinterfaces, ontoereikende encryptie)	●	●	●
• Bekende zwakheden in webapplicaties (o.a. SQL injection, XSS)	○	●	●
• Handmatig testen op specifieke functies in webapplicaties	○	●	●
• Zwakheden in business logica van webapplicaties (o.a. privilege escalatie)	○	○	●
• Volledige handmatige tests van de webapplicatie inclusief de business logica	○	○	●
Rapportage via Security Dashboard	●	●	●

Security Dashboard





Waarom Deloitte?

Deloitte heeft ruime ervaring op het gebied van het adviseren en beoordelen van de informatiebeveiliging binnen overheden en het bedrijfsleven. Ons team bestaat uit meer dan 40 specialisten die “ethical hacking” als hun grote passie omschrijven. De kennis, ervaring en passie is nogmaals bevestigd bij de finale van de Global Cyberlympics. Het team van Deloitte Nederland heeft in 2011 tot 2013 drie keer de hoofdprijs en in 2014 de tweede prijs in de wacht gesleept in een wedstrijd die bestond uit zowel offensieve als defensieve security uitdagingen.

Volgens het Forrester rapport “The Forrester Wave™, Information Security Consulting Services, Q1 2013, blijft Deloitte toonaangevend, met buitengewone feedback van haar cliënten. Bovendien, aldus het rapport, behaalde Deloitte de hoogste score waar het ging om uitvoerend vermogen.

Naast Forrester, heeft ook Gartner Deloitte, op basis van uitvoerende capaciteiten, benoemd als “Leader” in Gartners Magic Quadrant voor Global Risk Management Consulting Services.

Kortom, Deloitte is uw ideale partner om u te ondersteunen om uw bedrijfsdoelstellingen te halen door het maximale rendement te halen uit uw online activiteiten.

Contact

Wilt u een verbeterd inzicht in de beveiliging van uw online presence? Neem dan contact op met:

Coen Steenbeek
telefoon: +31 (0) 6 1234 2957
e-mail: csteenbeek@deloitte.nl
website: www.hackingasaservice.com