Wat is ethical hacking?
Waarom is het zo belangrijk voor jouw bedrijf?

Deze whitepaper is een gezamenlijke publicatie van Nucleus, Toreon en Intigriti.

Ethical hacking: 6 dingen die je zeker moet weten

Je leest dit eBook omdat je meer inzicht wil krijgen in ethical hacking. Daarom hebben we in dit hoofdstuk de meest voorkomende vragen over ethical hacking gebundeld. Zo heb je meteen een goede basis om de rest van dit eBook te lezen.

Wat is een ethical hacker?

Een ethical hacker is iemand die fouten en beveiligingsproblemen opspoort in systemen, netwerken, applicaties en servers van bedrijven. Dit gebeurt op vraag van het bedrijf in kwestie. Het doel van ethical hacking is altijd hetzelfde: de IT-security verbeteren.

Wat betekenen de termen white hat, grey hat en black hat als het over hackers gaat?

De black hat is de hacker die iedereen – mede dankzij de media - het beste kent: een crimineel die systemen hackt of misbruikt om er persoonlijk voordeel uit te halen. Denk bijvoorbeeld aan het stelen van persoonsgegevens of financiële gegevens, het uitvoeren van DDoS-aanvallen of het verspreiden van ransomware.

De white hat staat lijnrecht tegenover de black hat. Het is een ethical hacker die opereert binnen de grenzen van de wet en als doel heeft om de IT-security van bedrijven te verbeteren. Wanneer hij kwetsbaarheden ontdekt zal hij het bedrijf in kwestie daarvan op de hoogte brengen zonder de kwetsbaarheden publiek te maken. Op die manier kan het bedrijf de lekken dichten zonder gevaar te lopen.

De gray hat zit tussen de twee. Hij is niet noodzakelijk een crimineel die uit is op persoonlijk voordeel, maar hij houdt zich ook niet noodzakelijk aan de wet. Gray hat hackers zijn vaak op zoek naar erkenning en willen uitpakken met hun vaardigheden en expertise. Daarbij zetten ze bedrijven soms onder druk met deadlines waarop ze een bepaalde kwetsbaarheid publiek maken. Als het bedrijf niet snel genoeg met een oplossing komt, impliceert dat dus een groot risico.

Is ethical hacking iets voor mijn bedrijf of organisatie?

Ethical hacking kan gebruikt worden om verschillende redenen. Voor een aantal bedrijven is het een finale test. Ze zijn ervan overtuigd dat ze hun IT security helemaal op orde hebben en willen ethical hackers laten testen of dat ook écht zo is. Andere bedrijven kiezen dan weer voor ethical hacking omdat ze niet weet waar eerst beginnen. Dan wordt het rapport eigenlijk een soort roadmap voor security. Soms wordt ethical hacking echter ook gebruikt om het senior management het belang te laten inzien van een hoger budget voor security bijvoorbeeld.

De belangrijkste vraag die je moet stellen is vooral hoe kritisch je IT-infrastructuur, je applicaties en je data zijn voor je bedrijfsprocessen en je financiële resultaten. Wij merken dat IT voor het gros van de bedrijven vandaag bedrijfskritisch of op zijn minst erg belangrijk geworden is. Met andere woorden: ethical hacking is iets wat het merendeel van de bedrijven – ongeacht hun omvang of sector - zeker moet overwegen.

Waar vind ik ethical hackers?

Om een ethical hacker in te huren zet je best geen advertentie. Je moet gelukkig ook niet het Dark Web op om er te vinden. Er zijn vandaag heel wat gerenommeerde en betrouwbare IT-securitybedrijven die ethical hacking aanbieden als een service.

Toreon is daar een mooi voorbeeld van. Zij hebben experts in dienst die hun sporen verdiend hebben en die ze kunnen inzetten voor dit soort opdrachten.

Als je liever niet met één specifieke partner werkt, kan je terecht op een bug bounty platform als intigriti. Zij brengen je in contact met ethical hackers en leiden alles in goede banen.

Wat doet een ethical hacker?

Ethical hackers werken op verschillende manieren. Het begint wanneer een bedrijf de vraag stelt om hun applicatie(s) of infrastructuur tegen het licht te houden. Op dat moment zal een ethical hacker op basis van zijn expertise en met gebruik van een aantal specifieke tools en vaardigheden op zoek gaan naar kwetsbaarheden bij de klant.

Een Ethical hacker doen heel veel verschillende dingen. Een korte greep uit het aanbod:

- Controleren van systemen, servers, netwerken en applicaties op zwakke plekken
- Uitvoeren van pentests
- Uitvoeren van risicoanalyses
- Reviewen van code
- Rapporteren van bevindingen uit onderzoek
- Formuleren van aanbevelingen om fouten en kwetsbaarheden op te lossen
- Implementeren van oplossingen om de veiligheid te waarborgen
- Begeleiden en trainen van software developers bij het ontwikkelen van veilige code

Concreet maken klanten meestal een keuze tussen een penetratietest (meestal afgekort naar pentest) of het gebruik van een bug bounty platform.

Wat is een pentest en wat is bug bounty?

Bij de penetratietest wordt er een duidelijke timing afgesproken tussen klant en ethical hacker(s), waarbinnen de hacker de systemen zal controleren/hacken. Achteraf wordt er een rapport opgeleverd van de werkzaamheden en eventuele kwetsbaarheden. Meestal

wordt meteen ook een advies geleverd om het probleem aan te pakken. In sommige gevallen voeren ethical hackers zelf de vereiste beveiligingsoplossingen uit en/of leiden ze intern personeel op om beveiligingsproblematiek te voorkomen. Dit soort pentest wordt meestal uitgevoerd door experts die in dienst zijn van IT-securitybedrijven.

Bij een bug bounty platform maakt een klant gebruik van een platform waar ethical hackers zich beschikbaar stellen om websites te hacken. Meestal worden daarbij vooraf een duidelijke scope en bepaalde bedragen afgesproken die de klant uitbetaalt voor gevonden kwetsbaarheden. Dat bedrag is meestal afhankelijk van hoe kritisch een kwetsbaarheid is. De eigenaar van het platform controleert de kwetsbaarheid en levert een rapport. De ethical hackers op zo'n platform zijn meestal van diverse pluimage: full-time hackers, ervaren security-experts, studenten informatica, freelance IT-ers die graag wat extra geld verdienen, enz. Heel wat bedrijven en online platformen, zoals Facebook, Intel, Apple en Github bijvoorbeeld, hebben overigens een eigen bug bounty programma.

In latere hoofdstukken gaan we dieper in op zowel de pentest als het bug bounty platform.

Waarom is ethical hacking belangrijk voor jouw bedrijf?

IT security is een van de belangrijkste uitdagingen waar bedrijven – en meer specifiek CIO's en IT-managers – momenteel mee kampen.

De cijfers en trends zijn dan ook niet bepaald bemoedigend. In 2017 hadden we met Wannacry de grootste ransomware-aanval ooit en zagen we bij Telenet bijvoorbeeld een stijging van het aantal aanvallen met 25%. 2018 was nog maar net gestart of we werden al geconfronteerd met de Meltdown en Spectre kwetsbaarheden… en pogingen om die te misbruiken.

Het is duidelijk dat cyberaanvallen vandaag voor veel bedrijven een harde realiteit zijn geworden. En dat ook cybersecurity dus heel serieus genomen moet worden.

De voordelen van ethical hacking

Elke security-expert haalt het aan: er bestaat niet zoiets als 100% security. Er is altijd een kans dat personen met slechte bedoelingen toegang krijgen tot je systemen of je data. Maar dat wil niet zeggen dat je niet kan proberen om het ze zo moeilijk mogelijk te maken.

Om te beginnen door onze securitymaatregelen op niveau te brengen en te houden uiteraard. Maar daarnaast ook door mensen in te schakelen die denken als hackers en die dezelfde methodes gebruiken als hackers. Het inzetten van ethical hackers biedt een aantal belangrijke voordelen:

- Je krijgt een uitgebreide externe kijk op je IT security
- Je kan kijken hoe je aanvallen van buitenaf opvangt zonder enige risico te lopen
- Je krijgt een beter inzicht in de zwakke plekken binnen je IT-omgeving
- Je krijgt een beter inzicht in de technieken en tools die hackers gebruiken
- Je bent beter voorbereid op effectieve aanvallen van kwaadwillige hackers
- Je hebt de kans/tijd om je infrastructuur en applicaties veiliger te maken
- Je creëert bewustwording rond security bij al je medewerkers

De nadelen van ethical hacking

Zijn er ook nadelen verbonden aan ethical hacking? Wanneer je met betrouwbare partijen werkt niet, wanneer je zelf op zoek gaat naar iemand om in te huren of vast in dienst te nemen uiteraard wel. Want hoe je het draait of keert blijft ethical hacking nog steeds hacking. Iemand probeert toegang te krijgen tot je systemen of je data. Met alle risico's van dien. Je wil dus dat de persoon die dat doet niet 100% maar 110% betrouwbaar is.

Kan je het veroorloven om het niet te doen?

Meer dan naar de voordelen en nadelen te kijken, moet je je misschien de vraag stellen of je het je vandaag nog kan veroorloven om het niet te doen. De risico's – zowel financieel als qua reputatie – die een datalek of een geslaagde hack met zich meebrengen zijn zo groot geworden dat ethical hacking allicht een te verantwoorden investering is. Zelfs voor middelgrote en kleine bedrijven.

10 dingen die je moet doen voor je ethical hacking overweegt

Ethical hacking legt pijnpunten en kwetsbaarheden bloot in je infrastructuur of je applicaties. Het is dus sowieso een goed idee om je security op punt te hebben voor je hackers aanspreekt. Zeker ook omdat je ethical hackers betaalt – fixed fee, per uur of per gevonden fout – en je dus het kostenplaatje kan beperken door je security op orde te hebben. We geven je een stappenplan van dingen die je zeker moet doen voor je denkt aan ethical hacking.

1. Analyseer de risico's

De eerste stap is een grondige risico-analyse uit te voeren. Je gaat met andere woorden kijken welke kwetsbaarheden er nog aanwezig zijn in je bedrijf. Controleer daarbij uiteraard aan de infrastructuur en de applicaties, maar evengoed aan andere risicofactoren. Denk bijvoorbeeld aan toegangsprocedures (zowel fysiek als online), medewerkers (hackers gebruiken maar wat graag phishingtechnieken of social engineering) of bedrijfsprocessen.

2. Bekijk wie betrokken partij is

Ongetwijfeld is je bedrijf voor bepaalde dingen afhankelijk van derde partijen. Denk aan hardware- en softwareleveranciers, hosting providers, datacenters, enz. Jij kan je zaken perfect op orde hebben, maar toch in de problemen raken als een ander bedrijf het niet zo nauw neemt met security. Informeer daarom de betrokken partijen, zodat jullie de plannen op elkaar kunnen laten aansluiten.

3. Zorg voor een optimale set-up van je infrastructuur

Hoe stabieler, robuuster en veiliger je IT-infrastructuur is ontworpen en opgezet, hoe kleiner de kans dat je effectief in de problemen komt. Denk daarom aan security vanaf het moment dat je een systeem opzet of een applicatie ontwerpt. Security by design en by default is vandaag geen overbodige luxe.

4. Verzeker je van maximale fysieke security

De fysieke beveiliging van je servers vormt de eerste securitylaag. Wie kan het gebouw allemaal binnen? Hoe makkelijk is het voor niet bevoegde personen om toegang te krijgen tot je servers? Meestal is de fysieke beveiliging van servers in eigen beheer beduidend minder dan die van servers in een datacenter. Nucleus werkt bijvoorbeeld enkel vanuit Tier3++ datacenters: die hebben perimeterbewaking en 24/24u surveillance, toegangscontrole en camerabewaking. Daarnaast kunnen we servers in het datacenter zelf van elkaar scheiden via aparte afsluitbare ruimtes met eigen racks.

5. Beveilig je netwerk

De tweede laag van beveiliging is de netwerkbeveiliging. Dan spreken we in de eerste plaats over firewalls. Beperk je daarbij niet alleen tot de standaard packet-filtering firewall die bepaalt welk verkeer via welke poort mag passeren, maar installeer ook virtual firewalls die werken op het niveau van je virtuele machines zelf. Zo vermijd je dat een probleem op één machine zorgt voor problemen in je hele cluster. Doe dit overigens niet alleen voor inkomend, maar ook voor uitgaand verkeer. Daarnaast is ook een Intrusion Prevention & Intrusion Detection System (IPS/IDS) een must om ongewenste indringers op te sporen en buiten te houden. Als je daarnaast ook nog zorgt voor 24/7 monitoring en DDoS-bescherming, heb je netwerkbeveiliging goed gecoverd.

6. Bescherm je connecties

Je netwerk en je fysieke servers mogen dan veilig zijn, als je connectie dat niet is, loop je nog steeds grote risico's. Maak je gebruik van het internet om te verbinden? Gebruik dan Virtual Private Networks (VPN). Als je zeer gevoelige data of nood aan hoge bandbreedtes hebt, dan is een eigen point-to-pointverbinding via koper of glasvezel een absolute must.

7. Houd malware buiten

Naast fysieke beveiliging, netwerkbeveiliging en bescherming van je connecties, is er natuurlijk ook nog de beveiliging van je virtuele servers zelf. Denk daarbij bijvoorbeeld aan real-time malwarebescherming. En dan is er nog Log Inspection en Integrity Monitoring: regels opstellen die de identificatie van belangrijke security events vereenvoudigen en controleren of de configuraties en bestanden op je systeem nog altijd dezelfde zijn als bij de installatie.

8. Houd je security up-to-date

Wanneer je IT-security effectief goed geïmplementeerd is, kan je niet op je lauweren rusten. Goede security vereist nu eenmaal permanente opvolging. Daarom geloven wij bij Nucleus dat Uptime-as-a-Service de toekomst is: je besteedt het beheer, het onderhoud én de beveiliging van je infrastructuur uit aan experts. En in ruil krijg jij de garantie van maximale uptime en maximale security.

9. Maak je medewerkers continu bewust van het belang van security

Een van de belangrijkste kwetsbaarheden ligt niet noodzakelijk bij je infrastructuur of je applicaties. Het is geen nieuws dat medewerkers het soms niet zo nauw nemen met security (denk maar aan te eenvoudige wachtwoorden bv.) of gemakkelijk in de val kunnen gelokt worden via phishing of social engineering. Daarom is voortdurende training en bewustmaking een belangrijk aspect van je security.

10. Denk na hoe je wil betalen

Je kan een vast bedrag (fixed fee) afspreken, per uur werken of per gevonden fout (vaak het geval bij bug bounty). Bekijk wat het best is voor jouw bedrijf. Ben je niet zeker van je maturiteit op vlak van security, is een vast bedrag meestal de beste keuze.

Waar vind je ethical hackers? En hoe begin je eraan?

Je hebt beslist om ethical hackers in te zetten. Maar waar vind je die? En welke garanties mag je eisen en verwachten? Hoe ben je zeker dat je met de juiste partij in zee gaat?

Wie kies je voor bug bounty?

Als je kiest voor bug bounty is het relatief eenvoudig. Er zijn geen honderden kwalitatieve en betrouwbare platformen op de markt. Ofwel kies je voor een internationaal platform als HackerOne, ofwel voor een lokale variant als intigriti. Een lokale partner heeft als belangrijk voordeel dat je je contract en je rapporten face-to-face kan bespreken en er op elk moment terecht kan voor feedback.

Wie kies je voor pentesting?

Als je kiest voor pentesting is de keuze heel wat uitgebreider: heel wat IT-bedrijven, securityfirma's en consultancykantoren bieden die dienst aan. Drie belangrijke vragen kunnen je helpen bij je keuze.

1. Welke (technische) expertise krijg je?
Een pentester moet kwetsbaarheden in je netwerk vinden. Kennis, maar vooral expertise, is daarbij van groot belang. Kennis kan je controleren op basis van certificaten (zoals CEH, CISSP, enz.), expertise krijg je meestal bij senior profielen. Weet dus wie de test zal uitvoeren!

2. Ligt de focus op cybersecurity?
Cybersecurity moet de primaire focus zijn van je pentesting-partner. Consultants of IT-bedrijven die bijkomend ook pentests uitvoeren halen niet hetzelfde niveau als iemand die dagelijks enkel bezig is met cybersecurity.

3. Welke methodologie wordt gebruikt?
Vraag potentiële pentesters welke methodes en tools ze gebruiken. Beperken ze zich bijvoorbeeld tot een standaardmethode of hebben ze een eigen methode die bepaalde dingen combineert? Gebruiken ze bestaande tools of hebben ze er ook zelf ontwikkeld? Hoe meer er op maat van jouw bedrijf kan gewerkt worden, hoe beter.

5 stappen om te onthouden

Als je je keuze gemaakt hebt, zijn er nog een aantal stappen die je zeker moet overwegen voor, tijdens en na het project.

1. Bepaal een duidelijke scope én methode
Bepaal vooraf in overleg met de betrokkenen wat je getest wil hebben en wat niet. Dat bespaart je tijd, moeite én centen. Bekijk ook welke methode (pentesting, bug bounty, enz.) het beste past bij je noden.

2. Plan vooraf
Behandel een pentest of bug bounty program net als elk ander technisch project: trek er de nodige mensen, middelen en tijd voor uit. Besteed ook de nodige aandacht aan de vragen die de ethical hackers vooraf zullen hebben.

3. Breng de juiste mensen op de hoogte
Wanneer je mensen je system laat hacken, is het belangrijk dat de juiste mensen op de hoogte zijn. Als er een social engineering test is, bepaal dan vooraf wie daarvoor in aanmerking komt (zonder die mensen op de hoogte te brengen in dit geval).

4. Monitor je security
Je weet dat je gehackt zal worden. Is er een beter moment om te kijken of je bestaande security monitoring en alerts optimaal functioneren? Trek dus de nodige tijd uit om die in de gaten te houden tijdens de hacks.

5. Analyseer het rapport
Je zal heel wat informatie ontvangen. Neem de nodige tijd om die grondig te analyseren en te bespreken met de betrokkenen. Voorzie ook een debriefing met de ethical hackers en met je management om de resultaten te bespreken. Daarna kan je op basis van de resultaten én die besprekingen de nodige acties ondernemen.

Hoe werkt een ethical hacker?

Ethical hacking vraagt heel wat technische kennis en expertise. En uiteraard laten ethical hackers nooit helemaal in hun kaarten kijken. Maar we willen je toch proberen een beetje inzicht te geven in het eigenlijke werk.

Geautomatiseerde tools inzetten

Elke ethical hacker heeft zijn eigen tools. Dat kunnen tools zijn die al bestaan (vulnerability scans bijvoorbeeld) of die helemaal zelf ontwikkeld zijn. Die tools zorgen ervoor dat een deel van het werk geautomatiseerd kan worden, zodat de hacker zelf zich kan toeleggen op meer complexere methodes om kwetsbaarheden te vinden.

De resultaten die de tools opleveren worden meestal manueel nagekeken om er zeker van te zijn dat er geen false-positives zijn en om eventuele risico's verder te testen en te bevestigen. Er zijn natuurlijk ook zaken die niet automatisch getest kunnen worden.

Zwakke plekken vinden en uitbuiten

Een hacker zal in eerste instantie steeds op zoek gaan naar de zwakke punten in je infrastructuur. Door gebruik te maken van verschillende technieken en tools brengt hij alle toegangspunten in kaart en evalueert hij het niveau van veiligheid om zo zwakke plekken te vinden om uit te buiten. Deze werkwijze wordt herhaald tot het doelsysteem bereikt wordt.

Bij een inbraak gebeurt de initiële toegang dan ook meestal via niet-kritische componenten waar het niveau van veiligheid lager is. Vervolgens zal de hacker met behulp van "privilege escalation" en "lateral movement" techieken toegang proberen krijgen tot het eigenlijke doelwit.

Social Engineering & Phishing

Technologie wordt steeds complexer. Door deze verhoogde complexiteit is lang niet iedereen zich nog bewust van de risico's. De gebruiker wordt tegenwoordig dan ook vaak de zwakke schakel op vlak van security. We zien meer en meer dat de mens het doelwit is van cyberaanvallen.

Aanvallen gericht op gebruikers noemen we social engineering. Phishing is daarbij momenteel de meest voorkomende vorm. Hierbij tracht men aan de hand van een valse e-mail of een verzonnen verhaal, gegevens zoals wachtwoorden van nietsvermoedende gebruikers te ontfutselen om veiligheidsmaatregelen simpelweg te omzeilen.

Proof en traces verzamelen

Elke ethical hacker zorgt voor bewijsmateriaal (proof) en kan reconstrueren hoe hij de kwetsbaarheid ontdekt en gebruikt (trace). Log files en dergelijke kunnen gebruikt worden

om de acties te reconstrueren. Screenshots of ander bewijsmateriaal kunnen dan weer aantonen dat een hack geslaagd is.

Rapporten maken

Ethical hackers leveren meestal een rapport op. Bij bug bounty gaat het om de specifieke kwetsbaarheid die gevonden is en hoe die kan gereconstrueerd worden. Bij pentesting is het een uitgebreider rapport dat meestal uit volgende onderdelen bestaat:

- Management summary of executive summary: dit beschrijft in grote lijnen de bevindingen van de test en kan gebruikt worden om te rapporteren aan het (hoger) management
- Bevindingen: dit is een detailweergave van elk veiligheidsprobleem
- Impact: bij elke bevinding krijg je een score die de impact op de software/ het systeem aangeeft. Dit kan je gebruiken om aanbevelingen de juiste prioriteit te geven
- Aanbevelingen: je krijgt een aantal adviezen om zowel op korte als op lange termijn het niveau van je veiligheid te verbeteren
- Risicoscenario's: deze beschrijven manieren om kwetsbaarheden te combineren om een aanval te doen (meestal zijn dit de worst case scenario's)
- Derden: als je ernaar vraagt kan je ook een rapport voor derden krijgen dat de uiterst gevoelige technische details niet beschrijft, maar wel voldoende informatie weergeeft om te kunnen delen met derden

Wat is pentesting?

Met penetration testing of kortweg pentesting bedoelen we alle activiteiten die een inbraak door hackers simuleren. De doelstelling van een pentest is altijd hetzelfde: veiligheidsproblemen ontdekken en oplossen vooraleer kwaadwilligen ze kunnen misbruiken en schade aanrichten.

De meeste pentests zijn bedoeld om zoveel mogelijk kwetsbaarheden op te sporen en te rapporteren. Via security scans en allerlei tools wordt je infrastructuur en/of je applicaties uitgebreid getest. Elke kwetsbaarheid die de ethical hackers vinden, wordt ook gerapporteerd.

Een alternatief is dat je de ethical hackers een duidelijk doel geeft: het bemachtigen van een bepaald data record bijvoorbeeld. Het rapport dat volgt bevat dan de route(s) van inbraak. Bij deze pentest is het dus niet de bedoeling om zoveel mogelijk kwetsbaarheden te vinden, maar wel om net die te vinden om het doel te bereiken. Dit wordt ook wel "red teaming" genoemd.

Idealiter worden pentests uitgevoerd in een testomgeving en niet in de productie-omgeving. Er is altijd een kans dat de test een impact heeft op het systeem.

Hoe ziet zo'n pentest er concreet uit?

Bij een pentest heb je doorgaans een aantal duidelijk afgebakende fases.

Scoping
Tijdens de offertefase wordt de opdracht duidelijk gespecifieerd. Je spreekt duidelijk contractueel af wat de scope van de opdracht is, wat wel en niet getest mag worden en welke technieken toegelaten zijn. Afhankelijk van de inhoudelijke scope zal er ook een tijdsduur afgesproken worden (dit kan variëren van een paar dagen tot enkele weken).

Kick off
De kick-off meeting markeert de start van het project. Tijdens de kick-off meeting worden zowel de technische als de niet-technische vereisten van de opdracht besproken. Deze meeting wordt idealiter door alle stakeholders bijgewoond om de behoeftes zeker goed te capteren. Volgende zaken worden typisch tijdens de meeting besproken:

- De tijd en locatie van de pentest
- De technische contactpersonen
- De technische details van de opdracht
- De benodige voorbereiding
- Specifieke need-to-knows voor de opdracht

Er wordt ook steeds een NDA of authorisatieformulier ondertekend. Zonder mandaat is testen immers illegaal.

Voorbereiding
Ter voorbereiding van de eigenlijke pentest moet jouw technische contactpersoon samen met de ethical hackers een aantal stappen overlopen. Zo worden tussenliggende systemen en filters die zelf niet getest worden typisch uitgeschakeld voor de ethical hackers. Dit om zeker te zijn dat de doeltoepassing en systemen getest worden en niet de tussenliggende systemen. Verder worden bijvoorbeeld testaccounts uitgeprobeerd, om ervoor te zorgen dat ze zeker werken tijdens de test.

De pentest zelf
De pentest zelf verloopt volgens binnen de afgesproken scope. Hoe de ethical hacker daarbij te werk gaat en welk resultaat dat oplevert, bespraken we al in uitgebreid in het hoofdstuk "Hoe werkt een ethical hacker?".

Review meeting
Tijden de reviewmeeting of debriefing zal je samen met de ethical hackers het volledige rapport overlopen. Hier heb je de kans om verdere vragen te stellen.

Zijn er verschillende soorten pentests?

Er is niet één standaard pentest. Afhankelijk van de klant en de scope van het project kunnen specifieke pentests ingezet worden.

Application Penetration Test

Bij application penetration testing kunnen zowel zelf ontwikkelde applicaties als commerciële oplossingen onder de loep genomen worden. Dat kan voor desktop apps en mobiele apps. Het testen van een mobiele app is vrij specifiek en bestaat uit twee luiken. Een analyse van de veiligheid van de mobiele app zelf én een test van de webservices waarmee de app communiceert in de back-end. Het testen van de back-end webservices staat echter los van het mobiele platform waardoor elk platform hier baat bij heeft. Application Penetration Testing laat zelfs toe om APIs te gaan onderzoeken.

White Box Test

White box testen nemen een kijkje onder de motorkap van de software die getest wordt en gebruiken die kennis als onderdeel van het testproces. White-box testen zijn bijna altijd geautomatiseerd en vereisen interne kennis van de software en programmeervaardigheden.

Black Box Test

Bij Black box testen wordt software getest zonder vooraf de interne eigenschappen ervan te kennen. Deze tests maken gebruik van software-interfaces en proberen ervoor te zorgen dat alles werkt zoals verwacht. De tester weet met andere woorden wat het programma moet doen, maar weet niet hoe het werkt. Black-box testen zijn gebruikelijk bij bedrijven die testers in dienst hebben die niet noodzakelijk kunnen programmeren of code kunnen begrijpen. Voor dit soort testen kan men zich baseren op algemene lijsten van mogelijke aanvallen voor applicaties zoals de OWASP Top 10, de SANS Top 25 Software Errors en CAPEC (Common Attack Pattern Enumeration and Classification). Maar ook op specifieke lijsten voor mobiele apps zoals de OWASP Mobile Top 10.

Network Intrusion Test

Bij een network intrusion test wordt gekeken of er aan de hand van foute configuraties of gekende kwetsbaarheden, ongeautoriseerde toegang mogelijk is tot je netwerken en systemen. Een network intrusion test kan vanop een intern netwerk zoals een LAN of Wifi georganiseerd worden, of vanop internet. Bij een interne test wordt nagegaan hoe groot het risico is op inbraak bij toegang tot een intern netwerk. Bij een externe test wordt het gevaar van een externe dreiging (outsider threat) bepaald.

Phishing Test

Een phishing test bestaat steeds uit twee onderdelen, een e-mail bericht en een bijhorende landingspagina. Het bericht is bedoeld om de gebruiker te overtuigen om op een hyperlink te klikken die naar de landingspagina verwijst. Deze pagina nodigt de gebruiker uit om zijn/haar gegevens in te vullen. Het kan gaan om het inschrijven voor een nieuwsbrief, het verschaffen van persoonlijke gegevens voor een wedstrijd, of het inloggen op een ogenschijnlijk gekend platform zoals Office 365. De overtuigingskracht van de test zit hem in de geloofwaardigheid van het verhaal. In de achtergrond host de hacker de nodige infrastructuur om de acties van de gebruikers te capteren.

Code & Configuration Review

De veiligheid van je infrastructuur of applicaties kan ook op een passieve manier geëvalueerd worden door de configuratie van het systeem na te kijken en te vergelijken met hardening standaarden. Ook de broncode van een applicatie kan geëvalueerd worden om zo kwetsbaarheden te ontdekken. Hiervoor worden typisch SAST- en DAST-tools gebruikt. Ook de fysieke veiligheid kan getest of geëvalueerd worden door een walk-through te organiseren met securityprofessionals.

Wat is een bug bounty programma?

Simpel uitgelegd: bij een bug bounty programma doe je beroep op ethical hackers, zonder ze in te huren bij een specifiek bedrijf. Je werkt daarentegen samen met de (wereldwijde) community van ethical hackers, in de bug bounty wereld researchers genoemd, uit binnen- en buitenland. Vaak gaat het om securityspecialisten die door de dag werken als systeembeheerder, developer of penetration tester, maar na de uren nog graag wat bijverdienen. Mocht je meer zekerheid willen over wie bij jou gaat testen, dan kan je stellen dat er enkel mensen mogen deelnemen van wie de identiteit gekend is, of dat er enkel mensen uit België mogen deelnemen.

De researchers gaan dan met jouw toelating op zoek naar fouten en kwetsbaarheden in jouw infrastructuur of applicaties en krijgen in ruil voor de dingen die ze vinden een "bounty" oftewel een beloning. Dat kan gaan van een vermelding op je website tot een financiële som. Dat is een keuze die je zelf maakt.

Hoeveel kost een bug bounty programma?

Je kan het perfect houden bij een (publiekelijk) bedankje door middel van een vermelding op je website, een berichtje op LinkedIn of via een klassieke brief. Mocht je dit doen, wordt het wel geapprecieerd mocht je ook wat "swag" opsturen. Dat is promotiemateriaal van je bedrijf zoals t-shirts, stickers, gadgets, enz.

Houd er wel rekening mee dat bepaalde researchers je enkel aandacht geven als je effectief ook een financiële vergoeding aanbiedt. Sommigen zien dit immers niet als een hobby maar als een bijverdienste en zullen dus enkel werken op projecten met een financiële vergoeding.

De vergoeding is vaak afhankelijk van de ernst van de fout. Vindt de researcher een kleine fout, hangt er vaak een kleine vergoeding aan vast. Kan de researcher echter een manier vinden om gratis producten aan te schaffen of je hele klantendatabank uit te lezen, dan wil je allicht een grotere vergoeding daartegenover stellen.

Belangrijk om weten: een bug bounty programma toegankelijk is voor ieder budget. Je kan immers zelf bepalen welke beloningen je geeft wanneer een researcher een fout ontdekt. En uiteraard bepaal je zelf ook de scope van het onderzoek en het maximale budget.

Volg de regels

De bedoeling is dat de researchers niet in het wilde weg wat proberen "te hacken". Ze respecteren de richtlijnen die jij opstelt. Je nodigt ze uit om fouten of kwetsbaarheden te zoeken, vaak in productieomgevingen, die je zelf over het hoofd gezien hebt of die niet naar boven komen bij klassiekere vormen van security testing.

Een bug bounty programma is een manier van security testen die zeer aantrekkelijk is voor bedrijven die al op regelmatige basis securitytests hebben laten uitvoeren door externe partijen en hier goed in scoren, of voor bedrijven die op zoek zijn naar een ietwat andere manier om de security te testen.

Eigen bug bounty programma versus bug bounty platform

Wettelijk mag iedereen een bug bounty programma opzetten, zolang je voldoet aan bepaalde voorwaarden. Zo moet je bijvoorbeeld duidelijk adverteren dat je researchers de toelating geeft om te gaan zoeken naar fouten. Je moet ook communiceren wat die researchers exact mogen en niet mogen. Verder moet het duidelijk zijn op welke manier een researcher zijn bevindingen op een veilige manier kan overmaken aan het betrokken bedrijf. Ook over de beloningen ben je best duidelijk.

Eigen bug bounty programma

Je kan als bedrijf kiezen om zelf zo'n bug bounty programma op te zetten, alles zelf te coördineren en proberen ethical hackers naar je website te lokken. Bekende namen als Brussels Airlines, Colruyt en Kinepolis doen dat al. Maar anderzijds ook KMO's en start-ups als Woorank en Suivo.

War moet je op letten als je zelf zo'n bug bounty programma wil beginnen?

- Je moet een goede en duidelijke communicatie voeren tegenover researchers om hen te informeren over wat kan, wat niet kan en hoe ze best met jou kunnen communiceren.
- Je moet researchers attent maken op het bestaan van je project en hen blijven motiveren op ook op lange(re) termijn om te blijven zoeken naar fouten in jouw omgeving.
- Je moet rapporten kwalificeren en valideren om te zien of ze correct zijn en of de aangehaalde fouten al dan niet bekend zijn. Dat kost de nodige tijd en expertise.
- Je moet een systeem van vergoedingen opzetten dat ervoor zorgt dat de researchers tijdig en correct beloond worden.

Een bug bounty platform

Ee tweede mogelijkheid is dat je gebruik maakt van een bestaand bug bounty platform. Dat is typisch een derde partij die een platform host waar ethical hackers samenkomen en waar je als bedrijf kan aangeven dat je open staat voor bug bounty. De organisator zal dan alle bovenstaande punten afdekken en zorgt ervoor dat je makkelijk in contact komt met de juiste researchers. Je hebt qua platform de keuze tussen lokale of internationale spelers.

Deze platformen gaan verschillende klanten combineren waardoor al bovenstaande punten waarop je moet letten makkelijk opgevangen kunnen worden. Ze hebben een community manager aan boord, zorgen voor de promotie van je project en de uitbetalingen van de researchers. Jij krijgt enkel een factuur voor geleverde diensten.

Belangrijker is echter dat zij het kaf van het koren zullen scheiden voor jou: zij bieden een verificatie aan van ieder ontvangen rapport waardoor je enkel rapporten zal ontvangen die

correct zijn, nuttig zijn en uniek. Hierdoor zal je dus je nuttige tijd focussen op de juiste zaken.