Security Test

Onderzoek naar kwetsbaarheden via pentests, social engineering én phishing

Elke organisatie bezit waardevolle data die niet in de openbaarheid mag komen of door hackers mag worden gestolen. Om de beveiliging daarvan te garanderen zijn technische maatregelen genomen met behulp van firewalls, virusscanners en malwarefilters. Deze tools doen wat ze beloven, maar hackers zijn onvoorspelbaar én er worden dagelijks nieuwe kwetsbaarheden ontdekt in gebruikte hard- en software. Het is belangrijk dat je regelmatig controleert of jouw IT-infrastructuur nog voldoende veilig is. Een Security Test is een vorm van ethisch hacken waarbij hack pogingen worden gesimuleerd om kwetsbaarheden bloot te leggen, zodat duidelijk wordt welke onderdelen verbeterd dienen te worden. Vaak vinden deze tests plaats in de vorm van interne en externe pentests, maar ook middels social engineering én phishing. Het is dé methode om te onderzoeken waar mogelijke kwetsbaarheden zich bevinden en hoe hier misbruik van gemaakt kan worden.

Pentest

Een pentest, afgeleid van 'penetratietest', legt de zwakke plekken in de infrastructuur, het platform of (web)applicaties bloot en geeft je inzicht in de kwetsbaarheid van daarvan. Onze experts voeren een scala aan digitale inbraakpogingen uit die tot op het diepst mogelijke niveau de infrastructuur testen. Met een pentest zet je de eerste stap naar het beheersbaar maken van de aanwezige beveiligingsrisico's. Vanzelfsprekend doen wij dit zo voorzichtig dat bedrijfskritische processen daar geen hinder van ondervinden en houden we ons bij het testen aan voor jouw branche belangrijke richtlijnen.

Beveiligingsrisico's in beeld

Wij laten je zien waar en hoe je met succes kan worden aangevallen en adviseren je wat je daar het beste tegen kunt doen. Na de test heb je een beter beeld van de beveiligingsrisico's die je loopt. Een uitvoerig en duidelijk rapport geeft alle informatie. Bevindingen worden hierin geclassificeerd naar risicoprofiel, met aanbevelingen voor het aanpakken van de ontdekte kwetsbaarheden. Zodra je weet wat de kwetsbaarheden van je organisatie zijn, kun je de juiste maatregelen treffen om de beveiliging te verbeteren. Wij hebben de juiste ervaring, tools en gecertificeerde experts en zorgen er zo voor dat je actueel inzicht hebt in de kwetsbaarheden en risico's.

Een pentest in 4 stappen

Stap 1: Verkenning

De infrastructuur en gebruikte software worden in kaart gebracht en er wordt gezocht naar beschikbare toegangsmogelijkheden. Eventueel wordt er social engineering gebruikt; de techniek om van buitenaf vertrouwelijke informatie in te winnen bij medewerkers.

Stap 2: Planning

Als kwetsbaarheden en risico's gelokaliseerd zijn, is het zaak om hier een compleet beeld van te krijgen. Om welke systemen en applicaties gaat het? Wat voor gedrag nemen we waar en kunnen we hier gebruik ofwel misbruik van maken? Aan de hand van deze informatie wordt er een plan van aanpak voor de daadwerkelijke aanval gemaakt.

Stap 3: Aanval

In deze fase gaan we daadwerkelijk kwetsbaarheden uitbuiten. Hoe ver de pentest gaat is uiteraard volledig afhankelijk van jouw wensen. Elke succesvolle poging laat zien in hoeverre een aanvaller het netwerk kan infiltreren en tot welke data en systemen hij toegang krijgt.

Stap 4: Rapportage

Als afronding van de pentest worden alle gevonden kwetsbaarheden in kaart gebracht. Hierop volgt een advies met beveiligingsmaatregelen voor de aangetroffen zwakke punten.

claranet

Meer informatie:
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak:
040 - 239 3300 - verkoop@claranet.nl

Planning van de pentest

Een pentest is het meest effectief als hij ruim van tevoren gepland wordt zodat er voldoende tijd is voor een goede voorbereiding. Voor het uitvoeren van de pentest is het daarbij van belang om rekening te houden met de volgende vragen:

- Zijn er tijdstippen, momenten of periodes waarin niet getest mag worden, bijvoorbeeld het einde van de maand rondom salarisverwerking?
- Zijn er kritieke changes gepland in de infrastructuur, waardoor het testscenario aangepast moet worden?
- Wat is de doorlooptijd en wanneer moet de opdracht uiterlijk afgerond zijn?
- Wie is er op de hoogte van de pentest?

Verschillende pentests

We onderscheiden diverse soorten pentests, van blackbox tot whitebox, volledig afhankelijk van de hoeveelheid informatie die vooraf beschikbaar wordt gemaakt en het doel van de pentest:

Blackbox

In dit geval vallen onze onderzoekers jouw systemen aan zonder enige voorkennis over applicaties, servers en/of infrastructuur. Deze werkwijze benadert de aanval zoals een cybercrimineel dit ook zou doen en we gedragen ons ook als zodanig. Er wordt vooraf geen informatie verstrekt aan ons vanuit de organisatie. De doorlooptijd van de test is hierdoor vooraf moeilijk te voorspellen.

Greybox

Wij krijgen in dit geval beperkte informatie over de systemen van waaruit wij mogelijke kwetsbaarheden verder onderzoeken. Dit scenario komt overeen met een hacker die op enige wijze reeds toegang heeft tot uw systemen. Hierbij kan je denken aan malware of een geslaagde phishing-actie. Dit is een reëel scenario waarbij bijvoorbeeld een medewerker (onbedoeld) betrokken is bij een cyberaanval. De doorlooptijd van de test wordt hierdoor aanzienlijk verkort.

Whitebox

In het geval van een Whitebox-test hebben we vooraf (vertrouwelijke) informatie zoals functionele, technische en architectonische ontwerpen. In het geval van applicaties kunnen wij zelfs de beschikking hebben over de broncode die wij aan een inspectie onderwerpen. Zo kunnen we lekken vinden die anders, onder andere bij een blackbox-test, lastiger te vinden zouden zijn. Met deze methode kunnen kwetsbaarheden op een efficiënte wijze worden opgespoord en heeft de test een nog kortere doorlooptijd. Met de beschikbare informatie kunnen we ook adviseren over een betere beveiliging zonder een daadwerkelijk testscenario te hoeven doorlopen.

Richtlijnen en vrijwaring

Vanzelfsprekend voeren wij de pentests zo uit dat bedrijfskritische processen daar geen hinder van ondervinden en houden we ons bij het testen aan voor jouw branche belangrijke normen en richtlijnen. Je geeft ons vooraf, door middel van een vrijwaring, toestemming om jouw informatiesystemen te testen. Dit om te voorkomen dat wij ons schuldig maken aan computervredebreuk. Uiteraard wordt er extreem zorgvuldig met data omgegaan, volgens de afspraken in de vrijwaring.

Aanvullende diensten

Cybercriminelen laten zich niet zomaar uit het veld slaan indien de IT-infrastructuur volledig afgeschermd is en zoeken andere mogelijke ingangen. Daarom bieden we een aantal aanvullende diensten om inzicht te geven in een aantal specifieke risico's.

WIFI-analyse

Een draadloze verbinding kan een aanvaller direct toegang verschaffen tot het interne netwerk. In dat geval is de WIFI-verbinding de ideale sluiproute. Onze expert toetst uw WIFI-netwerk op kwetsbaarheden en geeft een advies hoe u de beveiliging van uw draadloze netwerk kunt optimaliseren.

Social engineering

Social engineering is een middel om de factor mens in de data-beveiliging te misbruiken om zo het beoogde doel te bereiken. De mens blijft altijd de zwakste schakel binnen een organisatie. Jouw medewerkers zijn beleefd en behulpzaam, maar dit levert ook risico's op. Met social engineering zoeken we de grenzen van het vertrouwen van de medewerkers op en proberen we zo ver als mogelijk binnen te dringen in jouw organisatie.

Phishingtest

Phishing is een populaire vorm van cybercrime, die steeds vaker door criminelen en andere kwaadwillenden wordt gebruikt. Via e-mail (of telefoon) wordt 'gefished' naar de inlog- en/of andere gebruikersgegevens. Een medewerker hoeft maar één verkeerde link aan te klikken en de gevolgens zijn niet te overzien. Phishingmails zijn bijna niet meer van echt te onderscheiden. Vroeger zag je aan de spelfouten en de opmaak nog wel dat er iets niet in de haak was, maar dat is al lang niet meer het geval. Onze phishingtest bestaat uit verschillende gradaties, waarbij je zelf kan bepalen welke onderdelen je wel en niet wenst. Met onze phishingtest kunnen we testen hoe vaak er op de link wordt geklikt, hoe vaak er wordt ingelogd en hoe vaak een besmette bijlage wordt gedownload.

Onze Social engeneering- en phishingtests zijn zo opgesteld om gedragsverandering van de medewerker meetbaar te maken. Het vergroot het bewustzijn van het risico bij de medewerkers en geeft een duidelijk vertrekpunt voor de organisatie. Je krijgt via een duidelijke rapportage inzicht in hoeverre het securitybeleid nageleefd wordt door de medewerkers en waar risico's zich bevinden. Hierdoor wordt je in staat gesteld om maatregelen te treffen en de beveiliging van jouw organisatie verder te versterken.

Garanties en voordelen:

Op maat gemaakt testscenario voor een specifieke vraagstelling
Onafhankelijke rapportage
Volledig overzicht van zwakten en kwetsbaarheden
Geeft houvast voor vervolgstappen in verbetering van beveiliging
Geeft inzicht of issues leiden tot een overtreding van de huidige databeveiligingsnormen
Kan worden ingezet samen met de Vulnerability Scanner
Maakt de organisatie en medewerkers bewust van kwetsbaarheden

claranet

Meer informatie:
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak:
040 - 239 3300 - verkoop@claranet.nl