Zoek uw kwetsbaarheden op voordat hackers dat doen

Het internet is nog steeds vergelijkbaar met het “Wilde Westen”, waar gekken en door de staat gesponsorde personen uw bedrijf stuk kunnen maken. Met een paar goed uitgevoerde toetsaanslagen nemen ze bezit van uw data. Of het nu om financiële informatie, systeem wachtwoorden of zeer belangrijke bedrijfsinformatie gaat, een datalek kan uw bedrijf blootstellen aan een aanzienlijk groot risico.

Er zijn veel manieren waardoor uw security maatregelen kunnen falen, daarom is het erg belangrijk dat er gedurende het testen ernstige kwetsbaarheden worden ontdekt. Het is dan ook van cruciaal belang uw security te laten testen door één van onze zeer ervaren security specialisten.

Met spriteCloud is en blijft uw bedrijf veilig. En natuurlijk zullen wij uiterst zorgvuldig omgaan met deze gevoelige informatie wanneer onze experts de kwetsbaarheden van uw bedrijf blootleggen.

Penetratietestservice

- Vulnerability scan
- Cyber bedreigingen (OSINT)
- Penetratietest van uw draadloos netwerk
- Penetratietest van uw webapplicaties
- Penetratietest van uw mobiele applicaties
- Penetratietest van uw infrastructuur

spriteCloud

Vulnerability scan

In tegenstelling tot een penetratietest die kwetsbaarheden probeert bloot te leggen zal een vulnerability scan veel meer potentiële kwetsbaarheden blootleggen in netwerk apparaten zoals routers, servers, firewalls en applicaties. Het uitvoeren van een vulnerability scan is qua kosten lager dan het uitvoeren van een penetratietest maar deze scan zal uitsluitend aantonen dat er mogelijke kwetsbaarheden aanwezig zijn, de scan zelf geeft geen gedetailleerde informatie over hoe dit zou kunnen worden uitgebuit. spriteCloud gebruikt uitsluitend tools die toegespitst zijn voor ondernemingen bij het uitvoeren van een vulnerability scan waardoor u verzekerd bent van de beste resultaten.
Omdat datalekken vaak het gevolg zijn van niet geïmplementeerde verbeteringen zal een vulnerability scan u een proactieve aanpak bieden voor het identificeren en elimineren van deze veiligheidslekken. Wij adviseren u om regelmatig vulnerability scans uit te (laten) voeren zodat u gevrijwaard blijft van nieuwe kwetsbaarheden. Op aanvraag kunnen wij u zowel scans zonder invoer van verificatiegegevens als met invoer van verificatiegegevens en zowel vanuit externe als ook interne perspectieven aanbieden.

Cyber bedreigingen (OSINT)

De intelligentie van Cyber bedreigingen maakt gebruik van de OSINT methodiek en omvat het verzamelen van informatie over uw organisatie uit openbare bronnen. Ons doel is om u te voorzien van een dreigingsevaluatie welke gebaseerd is op informatie waarvan bekend is dat hackers deze gebruiken. Deze informatie geeft uw inzicht over uw veiligheid na een eventuele efficiënte phishing aanval en na een sociale engineering campagne. Wij analyseren uw data en presenteren u een actieplan waarmee u zich uitstekend kunt beveiligen tegen Cyber bedreigingen.

Onze diensten omvatten het verzamelen van algemene informatie, het uitvoeren van een grondige netwerkanalyse door middel van dns- en sub domein opsommings technieken, het identificeren van de internet voetafdruk van uw organisatie inclusief informatie over belangrijke personeel- en broncode lekken en een niet invasieve behandeling om zwakke punten te ontdekken die zouden kunnen worden misbruikt.

Cyber aanvallen zijn in opkomst zelfs voor SMB's

"Tenzij u van plan bent om de wifi-netwerken in uw organisatie te elimineren, is het beoordelen van kwetsbaarheden van deze netwerken een must."

Penetratietest van uw draadloos netwerk

Draadloze communicatie is in onze moderne manier van leven essentieel, maar draadloze netwerken zijn één van de meest gebruikte ingangen van hackers om toegang te krijgen tot uw bedrijfsnetwerk. Draadloze netwerken zijn lastig om te controleren, te monitoren en te beschermen tegen indringers, dat is waarom draadloze netwerk security specialisten vaak worden ingehuurd door bedrijven om hun netwerk te testen.

Penetratietest van uw draadloos netwerk kan uw organisatie helpen in het voorkomen van drie zeer belangrijke kwesties:

- Hackers die uw draadloze netwerk gebruiken als ingang voor het binnendringen van uw organisatie
- Hackers die communicatie in hun eigen voordeel manipuleren
- De privacy van andere draadloze netwerk gebruikers wordt bedreigd

Onze penetratietest gericht op het draadloze netwerk is ontworpen volgens de nieuwste technieken om mogelijk kwetsbaarheden te ontdekken in WEP, WPA-PSK, WPA2, WPA3 gecodeerde netwerken. Ook worden mogelijk onbetrouwbare toegangspunten gecontroleerd (als er al toegang is afgedwongen). Dit kan ook gebruikt worden als een belangrijk hulpmiddel om het bewustzijn te vergroten van een effectief security protocol en het voorkomen van zeer kostbare beveiligings inbraken.

Penetratietest van uw webapplicaties

Een web applicatie penetratie test maakt gebruik van handmatige en geautomatiseerde hacks om bedreigingen op of kwetsbaarheden in uw webtoepassing te identificeren. Het doel van deze test is om kwetsbaarhedenen mogelijke dreigingen vast te stellen, en om toepassingen te vinden om ze af te zwakken over de gehele applicatie en de bijbehorende onderdelen (database, broncode, back-end services). Ons team met OSCE en OSCP gecertificeerde 'ethische hackers' gebruikt exploits (zoals SQL-injecties en XML External Entity (XXE) injecties) om voortdurend mogelijkheden te onderzoeken om controle te krijgen over uw webtoepassingom te voorkomen dat anderen dat doen. We bieden drie oplossingen:

Black-box

De tester wordt in de schoenen van een normale internetgebruiker geplaatst zonder enige kennis van de werking van de toepassing of zonder toegang tot de broncode. Deze methode komt het dichtst in de buurt van wat een echte hacker tegenkomt wanneer hij probeert uw applicatie te hacken.

Grey-box

Dit is een combinatie van Black-box en Clear-box testen, testers kunnen uitgebreide testen uitvoeren en toch dicht bij realistische hack mogelijkheden blijven. Testers beschikken over kennis van de interne werking en de functionaliteiten van de applicaties, maar hebben geen toegang tot de broncode.

Clear-box

Deze test benadering vereist dat de tester toegang heeft tot de broncode van de applicatie. Hierdoor kan de tester de kwaliteit van de code controleren, binnen een grotere scope die normaal gesproken door een ontwikkelaar wordt uitgevoerd. Hoewel het niet representatief is voor de omstandigheden in de praktijk, zorgt het wel voor een effectievere beveiliging.

Een enkele overtreding kan uw bedrijf vernietigen.

Penetratietest van uw infrastructuur

Met meerdere computersystemen, apparaten en gebruikers heeft uw infrastructuur veel mogelijke ingangen waar kwaadwillenden toegang zou kunnen krijgen en grote schade kunnen aanrichten. Onze infrastructuur penetratie testen geven u een voorsprong door u te helpen de mogelijke hiaten in uw beveiliging op te vullen en ervoor te zorgen dat uw klantgegevens, intellectuele eigendom en financiële informatie veilig blijven tegen bedreigingen, zowel vanuit extern als intern perspectief. Onze gecertificeerde security experts zijn getraind om u te helpen uw netwerk in een virtueel fort te veranderen.

We bieden twee benaderingen, een 'black-box' external infrastructure testing en internal ('a infrastructure testing.

External infrastructuur

Blootstellingen als gevolg van zwakke firewall configuraties, fouten in applicatiecode of patch problemen kunnen ervoor zorgen dat hackers toegang krijgen tot uw systeem. Een externe infrastructuur test helpt bij het identificeren van deze mogelijke ingangen en geeft aanbevelingen hoe ze kunnen worden beveiligd. Deze methode is een manier om na te bootsen hoe een hacker zonder kennis van het systeem je infrastructuur zou kunnen benaderen.

Internal infrastructuur ('veronderstelde inbreuk')

Een interne penetratie test kijkt naar beveiligingsproblemen binnen uw netwerk. Gesegmenteerde netwerken zorgen ervoor dat ontevreden werknemers of hackers die toegang hebben gekregen tot uw interne netwerk, worden beperkt in hun mogelijkheden. Deze interne netwerkaanvallen zijn net zo schadelijk als en vaker dan externe aanvallen. Deze opdrachten volgen de mindset van 'veronderstelde inbreuk' met behulp van het MITER ATT & CK-framework om beveiligingslekken en SOC-detectiemogelijkheden te testen.

"Uw informatie en die van uw klanten moeten privé worden gehouden. Uw reputatie en uw bedrijfsresultaten hangen ervan af."

Penetratietest van uw mobiele applicaties

Net zo snel als mobiele apparaten en mobiele toepassingen deel zijn geworden van het dagelijks leven, zo ook zijn de veiligheidsinbreuken en aanvallen op deze toepassingen zeer sterk in aantal gestegen. Een belangrijke oorzaak hiervan is de toegenomen tijdsdruk die ontwikkelaars tegenwoordig hebben om nieuwe functionaliteiten te maken en de apps zo snel mogelijk op de markt te brengen.

Al deze redenen maken het regelmatig uitvoeren van een penetratietest van uw mobiele toepassingen van cruciaal belang om de reputatie van uw app en uw bedrijf te blijven beschermen. Er is slechts één slechte recensie van de pers

Zijn uw applicaties, netwerken en systemen veilig? Nu is het de tijd om dit uit te vinden, voordat een hacker dit doet.

Neem nu contact op met spriteCloud voor meer informatie over hoe onze Security Test Services u kunt helpen uw organisatie en klanten beter te beveiligen.

Bel ons op +31 (0) 20 61 59 155 of stuur een e-mail naar info@spritecloud.com