

CGI Vulnerability Assessment Service



Experience the commitment®

CGI Vulnerability Assessment Service (CGI VAS) är en tjänst för att identifiera tekniska sårbarheter i befintliga IT-miljöer. Syftet är att minska riskerna för intrång eller oavsiktlig skadegörelse som kan påverka eller skada den egna verksamheten.

Med en världsledande skanningsteknologi, utfört av CGI:s certifierade säkerhetstekniker, ger vi våra kunder en tydlig och klar bild av hur de med enkla medel kan skydda sin IT-miljö och därmed minimera den finansiella, juridiska och operationella risken samt eventuell skada på varumärket.

Tjänsten är modulbyggd och vi kan erbjuda allt från en skanning av en server med en enkel rapport till återkommande skanningar av hela IT-miljöer med avrapportering alternativt djupare analyser av resultatet. Modulerna kan väljas och kombineras på olika sätt för att med mycket stor flexibilitet anpassas till kunders specifika krav.

CGI kan även erbjuda ett åtgärdsprogram baserat på resultatet av skanningen för att hantera befintliga risker och säkra upp IT-miljön.

Sårbarhetsskanning med sårbarhetsbevakning

Genom att utföra en sårbarhetsskanning på överenskommen IT-miljö hjälper CGI till att identifiera tekniska sårbarheter och bidrar på så sätt till att kunna reducera risken i IT-miljön. Programvaran som används baseras på stora databaser med existerande kända sårbarheter (över 40 000).

Med hjälp av automatisk sårbarhetsbevakning kan CGI hjälpa organisationer att effektivt jämföra nyupptäckta sårbarheter mot tidigare insamlat resultat från den senaste skanningen utan att göra en ny skanning. Denna unika teknik för omvärldsbevakning av sårbarheter som uppstår i kunders miljöer, kallad "scanning-less-scanning", hjälper till att minimera tiden då säkerhetshål är exponerade och utan åtgärd.

TJÄNSTER OCH PRODUKTER SOM KAN KOMBINERAS MED CGI VAS

Risikanalyser

Ett rekommenderat sätt att börja säkerhetsfokuseringen är med en närmare undersökning av riskerna som berör organisationen. CGI kan erbjuda en komplett riskanalys för ett valt område, exempelvis ett IT-system eller en applikation. Vi kan leverera analyser som innehåller bland annat följande områden:

- Bedömning av aktuella hot och risker.
- Fastställande av sårbarheter.
- Framtagning av kostnadseffektiva åtgärder.
- Framtagning av en tydlig åtgärdsplan.

Minimera riskerna för intrång i din IT-miljö på ett enkelt och kostnadseffektivt sätt.



WEB APPLICATION ANALYSIS

- Hur säker är vår företagswebb?
- Skall vi oroa oss för DDOS och defacing?
- Är vår externa webb en språngbräda till företagshemlig information?

ANALYS AV EFTERLEVNADEN

- Uppfyller vår IT-miljö myndigheters krav?
- Kommer vi få nedslag på revisionen?
- Vad behöver vi åtgärda?

SECURITY HEALTH CHECK

- Är våra klienter rätt patchade?
- Har alla klienter FW och AV installerat?
- Hur stor är risken för interna attacker?

Webbapplikationsskanning

Majoriteten av attackerna mot IT-systemen utifrån utnyttjar nuförtiden svagheterna i webbapplikationerna. Därför behövs en alldeles speciell fokus just på detta område. Webbapplikationsskanningen...

- ... gör det möjligt för organisationer att bedöma, hantera och prioritera webbapplikationers sårbarheter.
- ... skannar både webbservern och applikationslagren i webbservern på ett unikt sätt.
- ... är enkel att sätta upp och använda. Det är ett mycket kostnadseffektivt sätt att bedöma webbapplikationer på en återkommande basis.
- ... snabbt och enkelt upptäcker attacker mot webbapplikationer genom att automatiskt skanna tusentals webbsidor efter sårbarheter.

Penetrationstester

Med hjälp av penetrationstester undersöker man IT-miljöns förmåga att stå emot obehörigas försök att komma åt interna system och data. Penetrationstesterna som genomförs manuellt av säkerhetsexperter har bl.a. följande fokusområden:

- Externa tester – de simulerade attackerna utförs från Internet.
- Interna tester – målet är att undersöka om t.ex. de anställda kan skaffa sig tillgång till data som de inte har behörighet till.
- Riktade insatser – testar sårbarheten hos kritiska system där ett intrång kan medföra stora konsekvenser.

Djupgående Analys

En djupgående analys av de framkomna resultaten samt en framtagna rekommendation till handlingsplan.

VARFÖR CGI

- ISO-certifierad spelare i säkerhetsbranschen med mångårig erfarenhet.
- Har både lokal och global närvaro.
- Har expertkompetens inom hela säkerhetsområdet.
- Har resurser att åtgärda identifierade sårbarheter om så önskas.

MER INFORMATION

Kontakta gärna våra representanter för mer information:

- Henrik Nordberg, tekniska frågor
henrik.nordberg@cgi.com
+46 8 671 20 00
- Tommy Magnusson, specialistsäljare
tommy.magnusson@cgi.com
+46 8 671 20 00

OM CGI

Grundat 1976, CGI tillhandahåller tjänster globalt inom IT och affärsprocesser genom att leverera affärsrådgivning av hög kvalitet, systemintegration och outsourcing. Med 72000 specialister i 40 länder är CGI ledande inom IT-industrin på att leverera projekt i tid och inom budget genom att anpassa våra team till kundernas affärsstrategier för att uppnå resultat över hela linjen.

För mer information om CGI, besök
www.cgi.com
eller mejla oss på info@cgi.com.