

OPRICHTING AMTSO IS DUIDELIJKE STAP VOORWAARTS

Het belang van goede testen

We gaan allebei alweer een tijdje mee in de industrie. Eén van onze terugkerende ergernissen zijn de slechte testen in verschillende bladen. En dan niet omdat de producten van onze bedrijven niet als eerste, of misschien zelfs als laatste zijn geëindigd, maar vanwege het ontbreken van veel benodigde gegevens bij de test. Vragen over de methodologie, welke versie er is getest en hoe de verschillende stukken malware zijn geselecteerd blijven vaak onbeantwoord. Dat dit een doorn in het oog is van de anti-malware producenten, zal duidelijk zijn, maar ook de testers zelf, de uitgevers en in toenemende mate de lezers ergeren zich hieraan. Binnen één en dezelfde maand kan product A zowel een test winnen bij tester X als verliezen bij tester Y.

TEKST: RIGHARD ZWIENENBERG
EN EDDY WILLEMS

Het is helaas zo dat er meer slechte tests zijn dan goede tests. De voortdurende strijd in deze arena heeft in geleid tot een positieve actie, de oprichting van AMTSO, de Anti Malware Testing Standards Organization. AMTSO heeft een aantal doelstellingen.

- Het leveren van een forum voor de discussies omtrent het testen.
- Het ontwikkelen en publiceren van objectieve standaarden en "best practices".
- Het promoten van educatie en het bewust zijn van problemen.
- Het leveren van utilities en bronnen die helpen bij standaardgebaseerde test-methodologieën.
- Het leveren van een analyse en overzichten van huidige en toekomstige testen van anti-malware en gerelateerde producten.

AMTSO is niet, in tegenstelling tot wat wordt beweerd, een organisatie die gedreven wordt door de anti-malware producenten. Alle belangrijke testorganen (zoals AV-Test, AV-Compatives en Virus Bulletin) en certificatie organen (onder andere ICSALabs, Westcoast Labs) werken samen in AMTSO. Om de objectiviteit te waarborgen is er ook een officieel Advisory Board, waar hoofdzakelijk academici en andere grootheden uit de beveiligingswereld in zitten.

AMTSO heeft niet als doel om te vertel-

len hoe er getest moet worden, maar wil er via gezamenlijk afgesproken standaard documenten voor zorgen dat de testen van anti-malware producten beter worden en dat de uiteindelijke testconclusie gestaafd is op de resultaten van de test en niet, bijvoorbeeld, op het advertentie budget.

Principes

Mochten wij in dit artikel de indruk wekken dat we enigszins bevooroordeeld zijn ten opzichte van AMTSO, dan is dat heel goed mogelijk. Righard is namens Norman in 2008 bij de oprichting van AMTSO betrokken geweest en daarna gekozen als President, en Eddy is namens G Data zeer actief binnen AMTSO. Na de oprichting van AMTSO is er eerst gewerkt aan het beschrijven van de fundamentele principes die met het testen van anti-malware producten nagestreefd moeten worden.

- Een test mag het publiek niet in gevaar brengen
- Een test mag niet bevooroordeeld zijn
- De test moet redelijk open en transparant zijn
- De effectiviteit en de resultaten moeten evenwichtig beoordeeld worden
- De tester moet genoeg zijn best hebben gedaan om te kijken of de samples in de test correct - geclassificeerd zijn als schadelijk, onschuldig of beschadigd
- De test methodologie moet consistent zijn met het doel van de test
- De conclusie van de test moet gebaseerd zijn op de resultaten
- De test resultaten moeten statistisch in orde zijn
- Producenten, testers en uitgevers moeten een duidelijk contactadres hebben voor correspondentie

Een gedetailleerde beschrijving van deze principes is te vinden in de documenten- sectie op de AMTSO website.

In de paar jaar dat AMTSO bestaat, zijn er al een heleboel documenten verschenen op de website. Hoe ben je bijvoorbeeld als tester zeker dat je goede virus samples gebruikt bij je testen? Een ander zeer belangrijk voorbeeld is hoe een tester te werk kan gaan bij het testen van in-the-cloud producten, waarbij de werkwijze



De Belg **Eddy Willems** is Security Evangelist bij G Data Software AG. Hij is al sinds 1989 actief op het gebied van IT-beveiliging. Tijdens die periode heeft hij gewerkt voor invloedrijke organisaties, zoals EICAR, waarvan hij medeoprichter en directeur pers en informatie is, verschillende CERT-instellingen, internationale politiediensten, de organisatie achter de WildList en commerciële ondernemingen zoals NOXS en Kaspersky Lab Benelux. Als Security Evangelist bij G Data vormt hij de link tussen de technische complexiteit van IT-beveiliging en de gebruiker.



Anti-Malware Testing Standards Organization

