Metodológia – základný kameň úspechu

Napriek tomu, že schopnosti konzultanta vykonávajúceho testovanie sú primárne postavené na jeho odbornosti, prístup k testovaniu by nemal byť postavený na jedincovi a závislý od neho. Najväčšiu časť testovania tvorí manuálna systematická analýza jednotlivých bezpečnostných opatrení. Tak ako aj pri iných činnostiach, pokiaľ sa niečo robí systematicky, najlepší spôsob je postupovať podľa konkrétneho plánu alebo metodológie. Vynechanie metodológie počas testovania môže znamenať nekonzistenciu testu. Počas testovania sa využívajú rôzne metodológie s cieľom poskytnúť klientovi najlepšie dostupné riešenie, ako napr. metodológia OSSTMM a OWASP a dokumenty National Institute of Standards and Technology (NIST). NIST pojednáva o penetračnom testovaní v dokumente Special Publication 800-42, Guideline on Network Security Testing. Aplikovanie týchto metodológií a štandardov poskytuje konzultantovi riadenú štruktúru jednotlivých oblastí, ktoré musia byť otestované tak, aby sa test vykonal komplexne a podľa najaktuálnejších dostupných informácií o problematike.

Výstupy

Najdôležitejšia fáza penetračných testov je prezentácia výstupov. Jednotlivé fázy testovania sú zdokumentované a detailne opísané. Tieto výstupy majú spravidla dve formy: súhrnná správa určená pre manažment a detailná správa určená pre technických pracovníkov.

Neoddeliteľnou súčasťou reportov sú inštrukcie, prípadne odporúčania, ako identifikovanú slabinu odstrániť, prípadne minimalizovať riziko jej zneužitia.

■ MARTIN BEŇUŠKA,
Security Consultant S&T Slovakia

Nový jazyk môže pomôcť pri programovaní pre viacjadrové procesory

V súčasnosti sa rozvíjajúce viacjadrové procesory dávajú programátorom k dispozícii vysoký výkon, potrebné je však zvládnuť paralelné programovanie. To môže byť pre programátora zložité a časovo náročné rovnako ako odhaľovanie prípadných programátorských chýb. Predpokladá sa, že bude treba paralelné programovanie zjednodušiť. Profesor Saman Amarasinghe spolu so svojimi kolegami z Computer Science and Artificial Intelligence Laboratory na Massachusetts Institute of Technology (MIT) preto už niekoľko rokov vyvíja riešenie v podobe nového programovacieho jazyka a jeho kompilátora s názvom StreamIT, ktorý pred programátorom ukrýva problémy paralelného programovania pri súčasnom využití jeho možností. V súčasnosti pracuje StreamIT na špecializovanom viacjadrovom stroji z dielne MIT, už v lete tohto roka by však malo byť k dispozícii riešenie pre čip Cell spoločností IBM, Toshiba a Sony, známy predovšetkým z hernej konzoly Playstation 3. Využívaná je paradigma data flow programovania, pri ktorej je priebeh výpočtov riadený nie tokom inštrukcií, ale dát, ktoré plynú funkciami. Programátor vytvára iba jednoduchý sekvenčný program, StreamIT dokáže posudzovať nezávislosť jednotlivých funkcií a rozdeľovať ich realizáciu jednotlivým jadrám bez obáv z prípadných závislostí alebo nebezpečenstiev, že by využívali tie isté časti pamäte a navzájom si tak prepisovali ich obsah.

REPORTÁŽ:

Infosec Europe

V dňoch 24. až 26. apríla sa v londýnskej hale Olympia stretli záujemcovia o bezpečnosť IT na 12. ročníku výstavy Infosec Europe. Na výstave predstavilo svoje produkty a riešenia 330 vystavovateľov. Počas tohto týždňa bolo pri príležitosti výstavy ohlásených 130 nových produktov a riešení. Stále sa prehlbujúci záujem o túto oblasti IT je podporený nárastom kybernetickej kriminality. Dnes, keď nie je veľký problém s relatívne nízkymi nákladmi sa dostať k firemným a chráneným informáciám, musia firmy a spoločnosti vynakladať čoraz viac prostriedkov na ochranu dát. A v skutočnosti je to kybernetický paradox.

Na výstave mali možnosť na jednej strane vystavovatelia riešení v bezpečnosti IT a na druhej strane záujemcovia o aplikovanie bezpečnostných riešení vymeniť si pohľady na problematiku a spôsoby jej riešenia. Okrem výstavnej plochy a stánkov jednotlivých firiem sa veľmi zaujímavé diskusie konali v konferenčných miestnostiach výstavnej haly. Najväčšiu pozornosť pútali prezentácie vrcholových manažérov firiem, ktoré udávajú trend a tvoria nové impulzy v oblasti bezpečnosti IT. Okrem kľúčových prednášok paralelne prebiehalo viac informačných línií. V New Product Theatre boli predstavované najzaujímavejšie novinky na výstave. V Implementation Forum Theatre boli prezentované a diskutované skúsenosti pri implementácii bezpečnostných produktov. Pre návštevníkov výstavy bola zriadená nová oddychová zóna, kde sa dalo v pohodlných kreslách príjemne oddýchnuť. Navyše sa tu cez interné TV kanály premietali na obrazovkách prednášky kľúčových rečníkov. S touto zónou susedila relaxačná časť pre návštevníkov, kde vám pomohli so stuhnutými krčnými stavcami, boľavým chrbtom alebo unavenými nohami.

Vráťme sa však k obsahu výstavy. Celej výstave dominovali riešenia na zabezpečenie koncových pracovných bodov používateľov. Keďže vo väčšine prípadov ide o notebooky, PDA, mobilné telefóny, kľúče USB a iné prenosné pamäťové zariadenia, prevažná väčšina riešení sa týkala týchto zariadení a spôsobu, ako zabezpečiť informácie v nich uložené a ako ošetriť prípady, keď sa zariadenia stratia alebo budú odcudzené, aby nedošlo k zneužitiu uložených dát. Druhý dominantný okruh riešení sa týkal autentifikácie používateľov, spôsobu jej uskutočnenia, administrovania a využitia na ďalšie a rozšírené poskytovanie služieb pre používateľov, ako napr. SSO (Single Sign On).

A treťou dôležitou oblasťou výstavy bola bezpečná komunikácia v sieťach s dôrazom na bezdrôtové riešenia a monitorovanie a správu siete z aspektu prehľadu o vykonávanej prevádzke v sieti a jej riadenia. Do tejto oblasti možno zaradiť aj riešenia na zabezpečenie internetového obchodu.

Popri výrobcoch produktov a poskytovateľoch bezpečnostných riešení sa na výstave zúčastnili aj asociácie združujúce odborných pracovníkov a špecialistov, ako ISACA, ISC2 a ISSA.

Lord Broers, člen Snemovne lordov a predseda Výboru pre vedu a technológiu

■ MILOSLAV DURČÍK, Londýn