informační
bulletin
AEC DATA SECURITY COMPANY

(Připravuje AEC Data Security Company – jakékoliv připomínky, náměty či dotazy posílejte na e-mailové adresy tomas.pribyl@aec.cz nebo petr.nadenicek@aec.cz)

Počítačové viry, antivirové technologie, elektronický podpis, šifrování dat – prostě ochrana datových informací vůbec.

Dnes přinášíme:

- ***Novinky mezi počítačovými viry: Shruggle***
- ***Novinky mezi počítačovými viry: Brador***
- ***F-Secure Windows XP Service Pack 2 Support Package***
- ***Několik vět o penetračních testech***

V průběhu září 2004 se pod taktovkou společnosti AEC uskutečnil další ročník akce AEC Roadshow. Tentokrát přednáškové turné zavítalo do Brna, Pardubic, Českých Budějovic, Liberce, Mostu a Zlína. Podrobnosti přineseme za měsíc.

AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Shruggle

Na konci srpna 2004 byl objeven virus Shruggle, o kterém některé zpravodajské weby informovaly jako o vůbec prvním viru pro 64bitové operační systémy. Přesnější informace ale správně uvádějí, že prvenství v této oblasti již patří jinému škodlivému kódu.

Shruggle opravdu je počítačový virus, který dokáže infikovat 64bitové spustitelné (PE - Portable Executable) soubory. Jedná se ale o první virus, který dokáže fungovat na Windows XP 64-Bit Edition na systémech na bázi AMD64. Jeho příbuznost s úplně prvním virem pro 64bitové systémy, kterým je virus Rugrat objevený v květnu 2004 se ale údajně zapřít nedá.

Kód viru není polymorfní, ani není žádným způsobem šifrován. Virus neinfikuje standardní 32bitové PE soubory ani nefunguje pod standardními 32bitovými operačními systémy (Windows 9x, NT, 2000 nebo XP) bez příslušné dodatečné podpory 64bitových aplikací.

Novinky mezi počítačovými viry: Brador

Brador je někdy označován za první backdoor pro PDA. Na infikovaném zařízení otevírá zadní vrátka na určitém TCP portu a informuje o tom svého „pána“. Jedná se ale pouze o škodlivý kód, který neobsahuje žádné funkce pro šíření vlastními silami.

Brador funguje pouze na systémech Pocket PC postavených na ARM architektuře s Windows Mobile 2003 (Windows CE 4.2) a novějších verzích. Na zařízení se kopíruje do adresáře Windows\StartUp pod názvem svchost.exe, čímž si zajišťuje svoje spuštění při každém re-startu PDA. Instalační rutina do zmíněného souboru zadních vrátek nepatrně zasahuje, čímž způsobuje jeho modifikaci při každém spuštění. Dosud se nepodařilo jednoznačně určit, zda se jedná o záměr autora kódu nebo o nechtěný vedlejší efekt. Po své instalaci backdoor zjišťuje lokální host IP adresu a odesílá ji e-mailem svému autorovi na určitou adresu. Když se tento e-mail podaří odeslat, backdoor otevírá TCP port 2989 a naslouchá na něm příkazům zvenčí.

Hacker se prostřednictvím tohoto otevřeného TCP portu může připojit k infikovanému PDA a převzít nad ním prostřednictvím zadních vrátek plnou kontrolu. Může být vzdáleně zneužit ke stažení i odeslání souboru z infikovaného PDA, případně ke spuštění dalšího kódu nebo zobrazení dialogových oken na PDA.

Odstranění lze provést vymazáním souboru zadních vrátek a restartováním PDA.

AEC
DATA SECURITY COMPANY

F-Secure Windows XP Service Pack 2 Support Package

Společnost F-Secure uvolnila informace o podpoře nedávno vydaného Service Pack 2 pro Windows XP a dala k dispozici několik servisních balíků pro některé své produkty.

Tento servisní balík vydaný společností F-Secure přidává podporu Windows XP SP2 do těchto produktů:

- **F-Secure Anti-Virus for Workstations 5.4x Windows XP SP 2 Support Package**
- **F-Secure Anti-Virus for Workstations 5.40-5.42**
- **F-Secure Internet Security 2003**
- **F-Secure Distributed Firewall 5.37 a novější**
- **F-Secure Workstation Suite verze obsahující F-Secure Anti-Virus nebo F-Secure Distributed Firewall 5.4x**
- **F-Secure Anti-Virus Client Security 5.5x Windows XP SP 2 Support Package**
- **F-Secure Anti-Virus Client Security 5.50-5.52**
- **F-Secure Internet Security 2004**

Obě dvě verze tohoto servisního balíku obsahují dvě základní funkce:

- **Podpora funkce „Data Execution Prevention“ ve Windows XP SP2 na hardwarové platformě procesorů AMD64.**
- **Podpora appletu „Security Center“ ve Windows XP SP2.**

Servisní balík je k dispozici pro následující produkty F-Secure:

- **F-Secure Anti-Virus for Workstations verze 5.40**
- **F-Secure Anti-Virus for Workstations verze 5.41**
- **F-Secure Anti-Virus for Workstations verze 5.42**
- **F-Secure Internet Security 2003**
- **F-Secure Anti-Virus 2003**
- **F-Secure Distributed Firewall verze 5.50 a novější**
- **F-Secure Workstation Suite verze obsahující FSAV 5.4x nebo FSDFW 5.4x**
- **F-Secure Anti-Virus Client Security verze 5.50**
- **F-Secure Anti-Virus Client Security verze 5.52**
- **F-Secure Internet Security 2004**
- **F-Secure Anti-Virus 2004**

Další informace najdete na stránkách F-Secure:
http://support.f-secure.com/enu/corporate/supportissue/general/xpsp2.shtml

AEC
DATA SECURITY COMPANY

Několik vět o penetračních testech

Bezpečnostní chyba v informačním systému, o níž nikdo neví, není nebezpečná. Pokud o ní ví administrátor či správce systému, stává se problémem který je zapotřebí urychleně řešit. Ovšem nejhorší variantou je situace, kdy o existenci chyby nebo nedostatku ví pouze potencionální útočník.

Jenomže jak v reálném světě chyby, které pro své útoky využívají právě hackeři či další nekalé živly, najít? Na tuto otázky není jednoznačná odpověď. Stejně je na tom zámek na dveřích, který je bezpečný do té doby, než jej někdo vylomí, a šifrovací algoritmus, který je bezpečný do té doby, než jej někdo „prolomí“. Jinými slovy: pozitivní důkaz se přináší těžko, negativní je naproti tomu nezvratný. Ve světě informačních technologií je to ale přece jen jednodušší. Existují metody, jak zjistit míru zabezpečení počítačů proti nejběžnějším typům útoků. Tyto totiž představují plus minus 99,99 procent všech napadení zvenku. Jednou z nich jsou penetrační testy.

Cílem penetračních testů je zjistit, do jaké míry je informační systém odolný vůči vnějšímu útoku. Zjednodušeně řečeno: v jejich průběhu dochází ke kontrolovanému napadení sítě a ke zjišťování slabých míst. Testy pracují na podobném principu jako třeba antivirové programy, které se v systému snaží nalézt viry na základě předdefinované databáze – při penetračních testech dochází k hledání známých bezpečnostních nedostatků na základě jejich předurčeného seznamu.

Externí penetrační testy jsou založeny především na cíleném vyhledávání možných bezpečnostních slabin informačního systému pomocí simulovaných útoků vedených na něj z internetu. Metodika tohoto druhu testů zpravidla obsahuje kontrolu bezpečnosti běžně používaných technologií. Zpravidla zahrnuje kontrolu:

- vstupní bodů do sítě (firewally, routery, paketové filtry aj.);
- demilitarizované zóny;
- otevřených portů;
- zranitelnosti služeb a aplikací (jako je web, DNS, FTP, SMTP, SQL a další internetové služby);
- zranitelnost pomocí DoS (resp. DDoS) či SynFlood útoků.

AEC
DATA SECURITY COMPANY

Penetrační testy provádí specializovaní dodavatelé zpravidla jako službu – příslušný software sice lze zakoupit, ale jeho pořízení, pravidelné aktualizování a vyškolení pracovníků je finančně nesmírně nákladné. K provedení penetračního testu zvenčí stačí zadat IP adresu zkoumaného systému (který ovšem musí být připojený prostřednictvím pevné linky – vytáčené linky mají adresu dynamicky přidělovanou, a tudíž měnící se) a podepsat smlouvu s příslušným poskytovatelem služeb.

Přitom tato smlouva je mnohem důležitější než by se na první pohled mohlo zdát. Poskytovatel penetrační služby se totiž na přání zákazníka stane „útočníkem“, který má za cíl zjistit slabá místa jeho sítě/systému při útoku zvenčí. Samozřejmě, že takovéto informace by se pak daly zneužít i k reálnému útoku – právě proto je dobrá smlouva oboustranně důležitá.

Pozor, provedení penetračního testu samo o sobě nedostatky systému neodstraní! V této fázi jsou potencionální slabá místa pouze odhalena – pokud možno dříve než na ně přijde útočník. Na provedení penetračních testů tak zákonitě musí navazovat fáze druhá – odstranění zjištěných bezpečnostních nedostatků (aplikace příslušných záplat, změna nastavení software…). Bez tohoto dokončení by penetrační testy neměly smysl.

Penetrační testy je dobré provádět opakovaně – jejich četnost pak závisí na konkrétním případu. Proč? Jednak se stále objevují nové a nové bezpečnostní chyby, na něž je potřeba systém otestovat. A jednak je tímto způsobem zpětně reflektován výsledek testu předchozího: zdali došlo či nedošlo k odstranění zjištěných slabin.

Suma sumárum: penetrační testy by měly být nezbytnou součástí provedení bezpečnostní analýzy informačního systému. Patří totiž k tomu nejlepšímu, co v současné době můžete pro bezpečnost své sítě udělat.

AEC
DATA SECURITY COMPANY