AEC Virus Eye

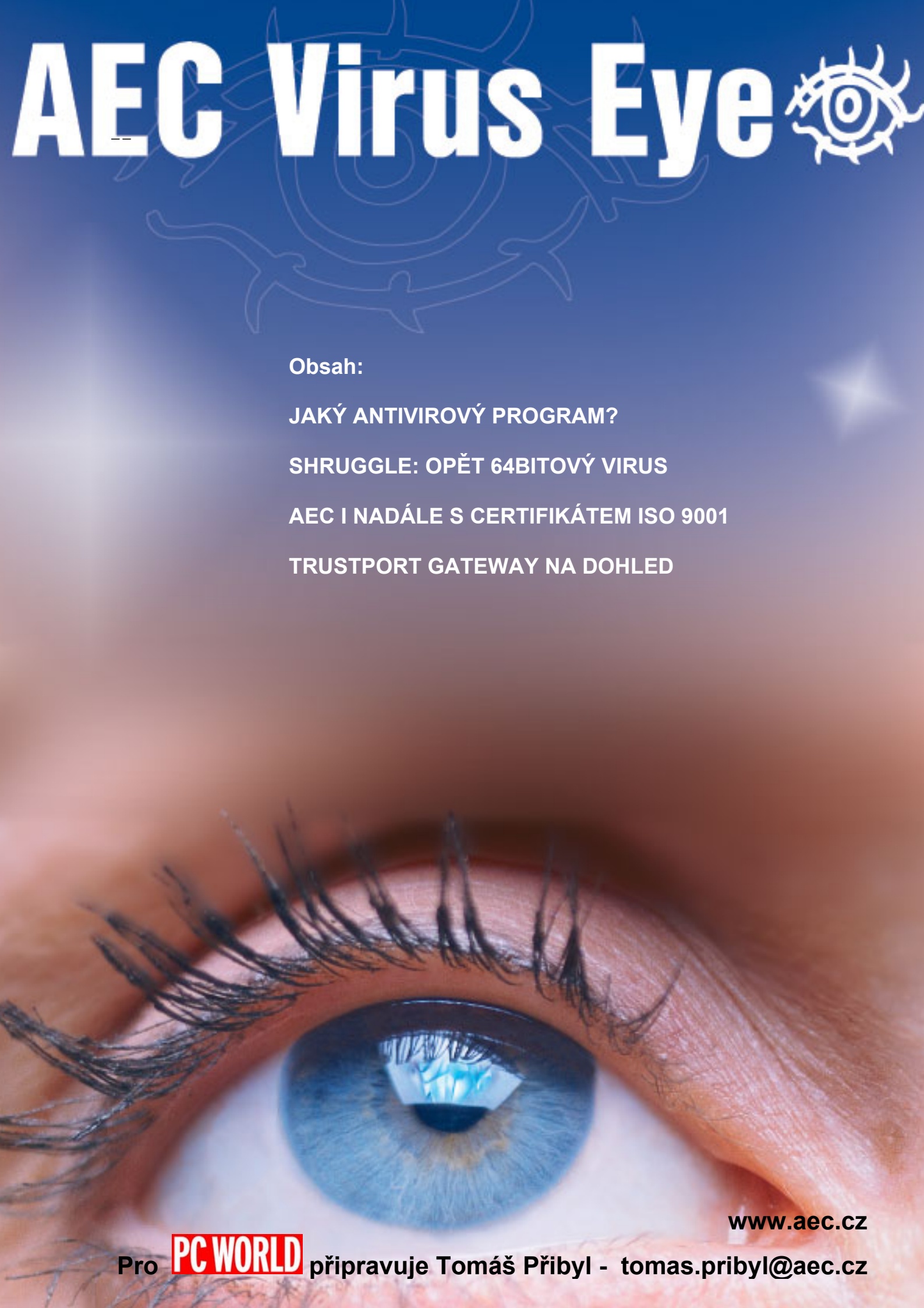
Obsah:

JAKÝ ANTIVIROVÝ PROGRAM?

SHRUGGLE: OPĚT 64BITOVÝ VIRUS

AEC I NADÁLE S CERTIFIKÁTEM ISO 9001

TRUSTPORT GATEWAY NA DOHLED



www.aec.cz

Pro PC WORLD připravuje Tomáš Přibyl - tomas.pribyl@aec.cz

JAKÝ ANTIVIROVÝ PROGRAM

Počítačové viry se staly běžnou součástí našeho života. Řečeno slovy klasika: „Můžeme s tím souhlasit, můžeme s tím, nesouhlasit, ale to je asi tak všechno, co s tím můžeme udělat." Antivirový program se tak stal nedílnou součástí vybavení každého počítače. Žádná sebepřísnější preventivní opatření totiž nikdy nedokáží zaručit stoprocentní bezpečnost. A navíc spoléhání se na vlastní síly a „šestý smysl" v době, kdy známe desítky tisíc virů, je přinejmenším bláhové.

Vzhledem k tomu, že nabídka antivirových programů je velmi široká, stojí uživatel před mnohdy nelehkou volbou. Který program je nejlepší? Který mě ochrání nejspolehlivěji? Na následujících řádcích nebudeme ukazovat na jeden konkrétní software, protože požadavky různých uživatelů jsou rozličné a každému z nich vyhovuje jiné řešení. Podíváme se ale na oblasti, podle nichž bychom si měli antivirový program vybírat.

Testy, recenze, doporučení

Jedním z nejsnáze dostupných zdrojů informací ohledně kvality počítačových programů jsou nejrůznější recenze a testy v časopisech či na webových stránkách. Otázkou je jejich skutečná vypovídací schopnost, neboť často odrážejí subjektivní zkušenosti a dojmy autora.

Mnohdy se různé antivirové firmy chlubí úspěšností v „lovu" počítačových virů v testech. Tady je ale jeden zásadní problém – testy mohou být velmi výrazně ovlivněny kvalitou použitých vzorků. Třeba na internetu lze nalézt desítky různých „studijních" databází, které zde umístili programátoři virů či nadšenci. Tyto jsou pak často novináři používané pro vytváření různých recenzí, ale… Praktická životaschopnost podobných „vzorků" v reálném světě bývá velmi diskutabilní. Ostatně, uvádí se, že k dnešnímu dni bylo vytvořeno nějakých 60 až 70 tisíc virů, ovšem reálně nebezpečný jsou asi jen dvě až tři stovky (které ale mají několik set dalších mutací). Jinými slovy: pokud antivirový program detekuje z nějaké databáze, kterou tvoří 15 tisíc virů, třeba 99,8 procenta kódů, může být v konečném důsledku stejně kvalitní jako software, který ze stejné databáze nalezne jen 65 procent.

Než dbát na různé recenze či testy (nikdo jim ale neupírá poradní hlas), je lepší se zeptat na doporučení přátel a známých. Vhodné také je několik antivirových programů si „osahat" – nainstalovat zkušební verze a měsíc je aktivně používat. Každému totiž vyhovuje něco jiného a nabídka na trhu

je dostatečně široká, takže není potřeba hledat zbytečné kompromisy.

Co všechno je potřeba chránit

Není počítačový virus jako počítačový virus. Stejně tak není antivirový program jako antivirový program. Jeden je silnější v chránění elektronické pošty, předností jiného je zase lepší schopnost odhalit v souborech i neznámé viry apod. Proto je dobré si zesumarizovat všechny požadavky, jaké na antivirový program máme. Samozřejmě je rozdíl mezi počítačem, který se denně používá k vyřizování e-mailové pošty a práci na internetu, a počítačem, který celoročně slouží k vedení účetní agendy a nová data (programy apod.) do něj vstupují jen výjimečně.

Ověřte si také, kde všude antivirový program vyhledává škodlivé kódy – poradí si třeba s archívy ZIP, ARJ, RAR…?

Krabice nebo služba?

Nejhorší věc, kterou lze udělat, je koupit si v obchodě za několik set korun krabici s antivirovým programem. Doma pak zjistíte, že při vyskytnutí problémů vám nikdo nepomůže, že nemáte nárok na aktualizace (velmi důležitá – viz níže), že program má ty a ty mouchy (třeba konflikt s lokálním softwarem či češtinou)…

Zkrátka a dobře: nikdy nekupujte antivirový program jako PRODUKT, ale vždy jako SLUŽBU. Třeba na rok, na dva, na tři… Po dobu trvání této služby máte nárok na antivirovou ochranu – na pravidelné aktualizace, na nové verze programu (pokud se objeví technologicky nový virus, což se čas od času stává), na technickou podporu…

Aktualizace – základ bezpečí

Svět počítačů má svá zvláštní pravidla a zákonitosti. Zatímco v reálném světě získáte jednou zakoupenou věc (většinou) již v provozuschopném stavu, o počítačové programy je zapotřebí se pečlivě starat – vyžadují aktualizaci, správná nastavení apod. V míře více než dvojnásobné to platí také pro antivirové programy.

Přitom v případě antivirových programů je zapotřebí rozlišovat hned dva pojmy – update a upgrade. Zatímco „update“ lze do češtiny přeložit jako „aktualizace“, s pojmem „upgrade“ je to trochu složitější a žádný jednoznačný ekvivalent pro něj

nemáme. Volně by sedalo říci, že „upgrade" je přechod na vyšší (tedy modernější) verzi daného produktu. Svým způsobem je to tedy také aktualizace, ale nikoliv dat, ale vlastního jádra antivirového programu.

Přestože jsou současné antivirové programy schopné se vypořádat i s mnoha neznámými viry (na základě sledování „podezřelých" příznaků apod.), přece jen je nutné poměrně často aktualizovat databáze virových řetězců – tedy jakousi kartotéku známých škodlivých kódů. To je dáno několika faktory – mj. antivirové programy jsou sice schopné různou „havěť" detekovat, ale bez detailnějších znalostí nejsou schopné čistit napadené soubory. Provádět aktualizaci se přitom doporučuje nejméně dvakrát do měsíce, v případě virových incidentů i častěji. Tři či čtyři měsíce neaktualizovaný program se považuje za starý a dodává uživateli pouze pocit falešné jistoty, nikoliv skutečnou ochranu.

Jak již bylo uvedeno, update je pouze dodání informací o nových virech do databáze příslušného programu, zatímco upgrade je vylepšení vlastního programu. Vzhledem k tomu, že se objevují stále nové a nové počítačové viry, je nutné škodlivé kódy hledat stále častěji i tam, kde to dříve nutné nebylo. Ruku v ruce s tím je zapotřebí vyvíjet i nové detekční algoritmy, které je nutné doplnit do jádra kontrolního programu.

Pro uživatele upgrade znamená mnohem více nepříjemností než update, neboť je mnohdy nutné původní program odinstalovat a nainstalovat jeho novou verzi. Je to ale jen jakési „nutné zlo" – daň za to, že jste pro ochranu svých dat udělali možné maximum.

Stoprocentní ochrana neexistuje…

Žádný antivirový program vám nedá stoprocentní záruku bezpečí a jistoty (a pokud někdo tvrdí, že ano, je to buď lhář nebo neví, o čem mluví). Pokud jej ale máte, správně používáte a navíc dodržujete určitá pravidla bezpečného chování s počítačem, můžete chodívat klidně spát. Riziko bezpečnostního incidentu je zanedbatelně malé…

SHRUGGLE: OPĚT 64BITOVÝ VIRUS

V úterý 24. srpna 2004 byl objeven virus Shruggle, o kterém některé zpravodajské zdroje 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 zapřít nedá.

Pokud je infikovaná aplikace spuštěna, infikuje Shruggle další 64 bitové spustitelné soubory v aktuálním adresáři. Infikování spočívá v jednoduchém přidání kódu viru, ve kterém je mimo jiné obsažen také následující text:

„Shrug - roy g biv“.

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.

AEC I NADÁLE S CERTIFIKÁTEM ISO 9001

Systém managementu jakosti společnosti AEC uspěl v pravidelném kontrolním auditu Lloyd´S Register Quality Assurance a může se i nadále honosit certifikací podle normy ISO 9001:2000. Ředitelka společnosti Ing. Alena Řezníčková k této události řekla: „Kvalitu v AEC chápeme především jako kvalitu našich služeb a spokojenost našich zákazníků. Jsme rádi, že i tento kontrolní audit potvrdil úspěšnost naší snahy v prosazování jakosti do všech činností firmy.“

TRUSTPORT GATEWAY NA DOHLED

Brány vývojového oddělení společnosti AEC opouští beta verze nového unikátního antivirového a antispamového řešení **TrustPort® Gateway.**

Již avizované řešení je modulární. Vyniká především rychlostí, jakou dokáže příchozí e-mailové zprávy kontrolovat. Je tedy vhodné pro ochranu všech poštovních serverů včetně těch s velkým provozním zatížením.

TrustPort® Gateway se skládá ze dvou základních částí:

- **TrustPort® Gateway Antispam** provádí antispamovou kontrolu na základě black listů, whitelistů a dalších běžných metod. Kromě toho může využívat také jedinečnou implementaci filtru s Bayesovou analýzou, který disponuje vlastní logikou a schopností učit se.

- **TrustPort® Gateway Antivirus** se stará o antivirovou kontrolu příchozí elektronické pošty. Modularita celého řešení umožňuje využívat kromě nového antivirového programu od společnosti AEC také další vhodné produkty, jako je třeba F-Secure Anti-Virus.

Řešení umožňuje využívat další zásuvné moduly, které rozšiřují možnosti zpracování příchozí pošty. Mohou provádět např. zálohování e-mailů apod. Další příjemnou vlastností řešení je možnost správy fronty čekajících e-mailů, což řeší problémy při stoprocentním vytížení serveru, který nezvládá dané zatížení. Všechny části sytému jsou výkonově škálovatelné. Pro každou část lze stanovit mohutnost paralelního zpracování.

Správa řešení je prováděna prostřednictvím webového grafického rozhraní, které pracuje na základě HTTP serveru se zabezpečením pomocí SSL.

Předpokládané uvedení TrustPort® Gateway na trh je v průběhu třetího kvartálu 2004.

[KONEC magazínu AEC VIRUS EYE]