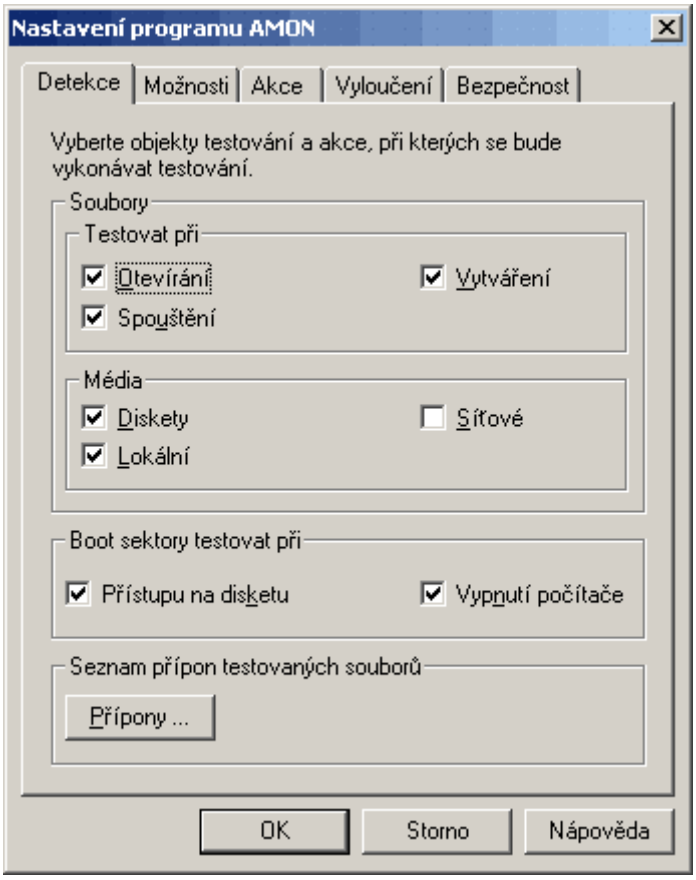
NOD32

Eset software

Tento dokument popisuje doporučená nastavení jednoho z nejlepších antivirových systémů.

Modul AMON

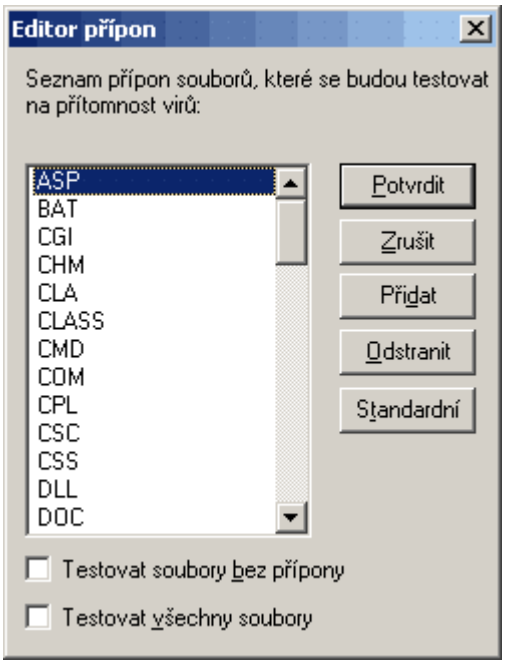
Tento modul se stará o testování souborů v okamžiku jejich použití. Od toho jeho název – Active Monitor. Je to jedna z nejdůležitějších částí antivirového programu. Bez ní by se dokázaly viry aktivovat bez vědomí uživatele.



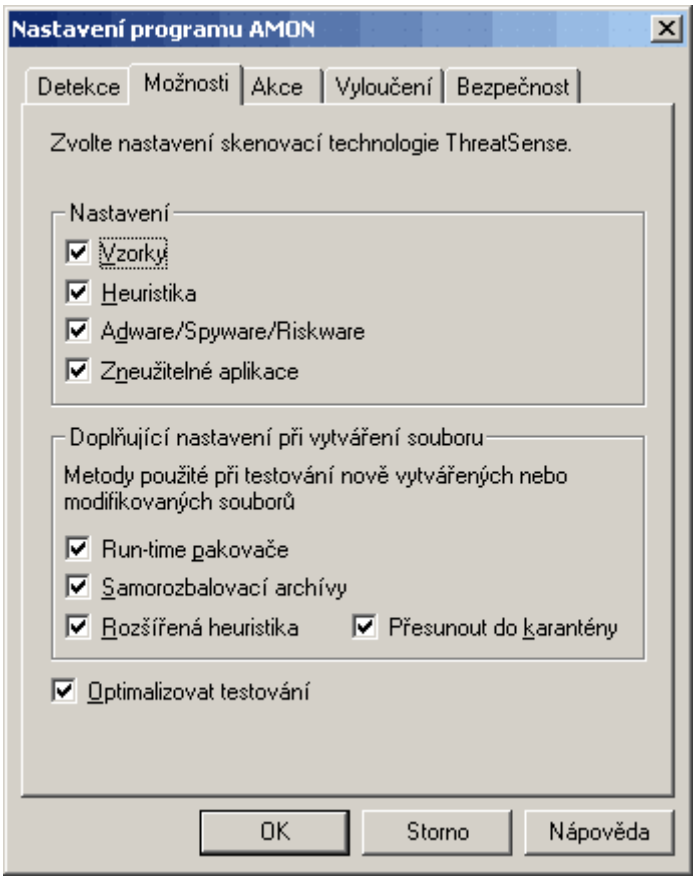
Testování při: Otevírání, Spouštění a Vytváření. Všechny tři volby jsou důležité. Některé viry jsou detekovatelné např. pouze při vytváření – při spuštění se snaží vytvořit vlastní kopii někde na disku a v ten okamžik je aktivní silnější detekce.

Média: Diskety a Lokální. Síťové nejsou nutné, zvlášť v případě, kdy se nepoužívá sdílení disků.

Boot sektory: poměrně důležité obě volby. Naštěstí se tyto viry ale již nešíří.



V tomto seznamu se určují přípony souborů, které se budou testovat v on-line režimu. Všechny tam nejsou proto, aby se ulehčilo počítači. V některých případech je vhodné odstranit příponu INI, některé programy využívají tyto soubory poměrně intenzivně (např. MoneyS3) a jejich kontrola zdržuje. Jedná se o konfigurační soubory, tj. jsou virově prakticky „nevyužitelné“.



Opět velice důležité nastavení. Zaškrtnuto musí být vše.

Vzorky: testuje „otisky“ známých virů. Nejspolehlivější, ale bohužel za tvůrcem viru logicky opožděná – nejdřív se virus musí na světě objevit, aby ho antivirové společnosti dokázali identifikovat.

Heuristika: zkusí si každý testovaný soubor spustit (bezpečně, jakoby „v sobě“) a hledá podezřelé operace v programu které jsou většinou výsadou virů. Bohužel to zvyšuje možnost planého poplachu, naštěstí ne výrazně.

Adware/Spyware/Riskware: touto volbou NOD nahrazuje funkce které byly donedávna výsadou programů typu Ad-Aware a jemu podobných. Nedá se říci, že by měl detekci lepší, přeci jenom specializovaný program na tom bude lépe, ale má neskonalou výhodu v tom, že je dokáže detekovat ihned při pokusu nakazit počítač.

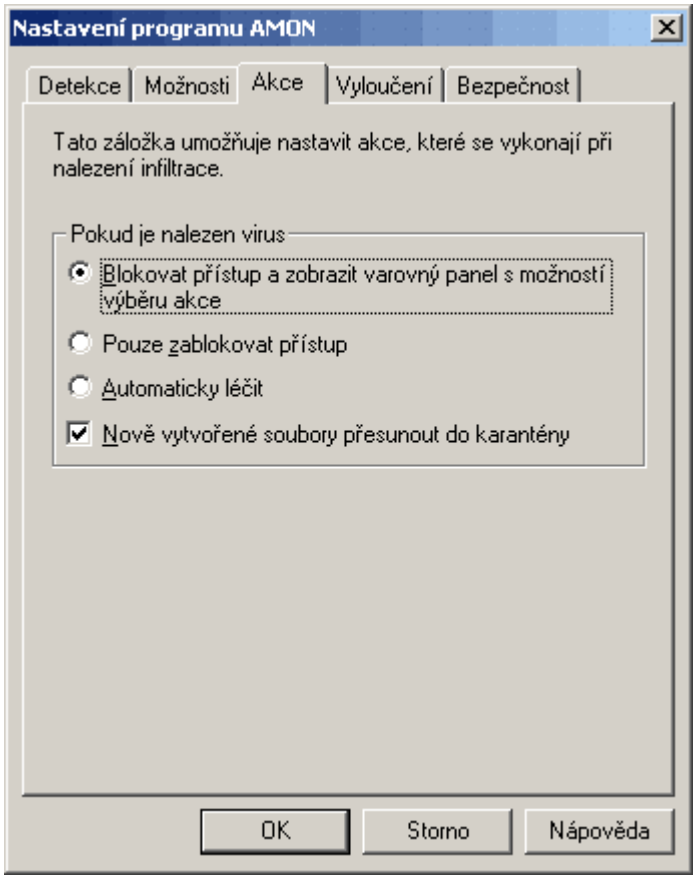
Zneužitelné aplikace: těžko říci, co tím autoři přesně myslí, ale mělo by to odchytávat programy typu backdoor (zadní vrátka). Nebo viz. nápověda – programy pro vzdálené ovládání počítače.

Doplňující nastavení při vytváření souboru:
Jak píšou v nápovědě – vytváření souboru si zaslouží extra nastavení, neboť většinou případné zdržení není poznat a co kdyby to náhodou vytvářel(o) nějaký virus na disku?

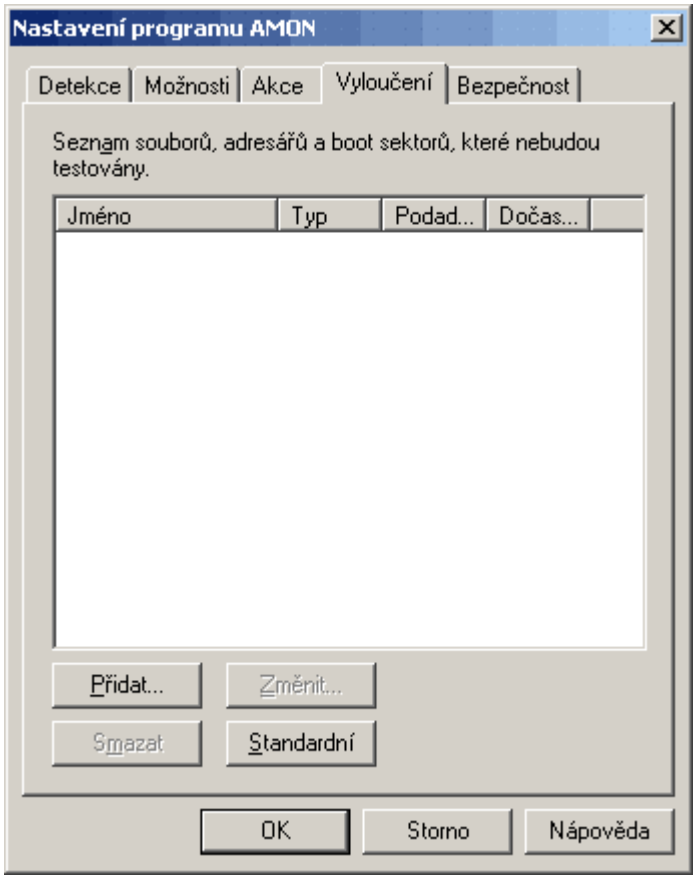
Run-time pakovače: velice důležité nastavení! Většina programů je interně komprimována (zabalena, něco jako ZIP) pro úsporu místa. Takže pokud je v programu vir, je možné, že je až v té zabalené části, takže není vidět. Tato volba si to nejdříve otestuje tak jak to je (aby nebyla nakažena ta rozbalovací část), potom si rozbalí vnitřek a testuje znovu.

Samorozbalovací archívy: platí pro ně to samé, co pro run-time. Tento archív totiž vypadá jako program, ale uvnitř může obsahovat programů několik.

Rozšířená heuristika: prostě důkladnější testování, jde „hlouběji“.



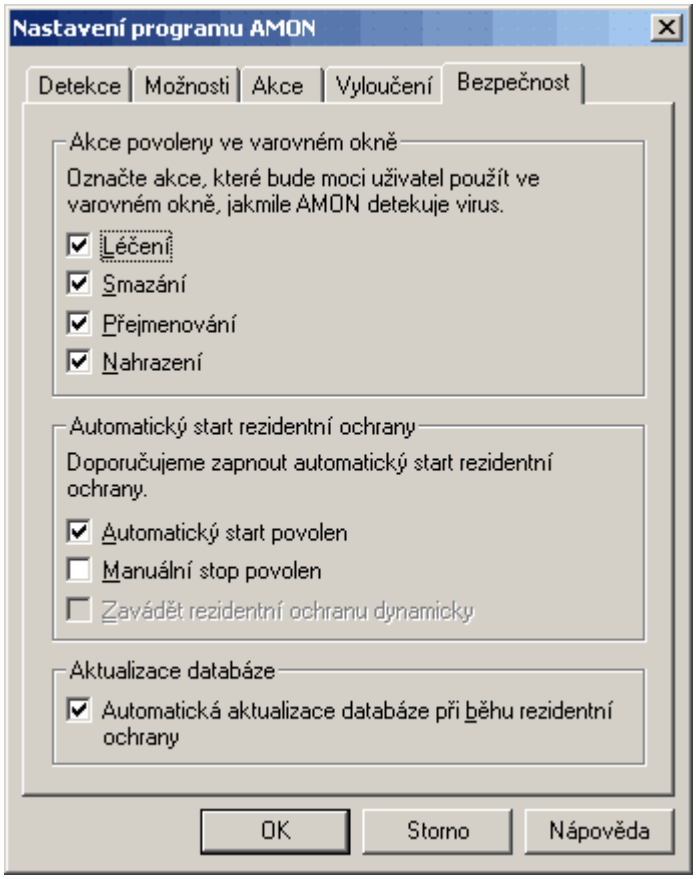
Toto nechte tak jak to je. Alespoň je vidět, že NOD něco chytil.



Zde lze vyloučit soubory z testování. Je možné tam vyjmenovat např. datové adresáře databázových programů (třeba účetnictví) u kterých je zaručena nemožnost nakažení (což u datových souborů je), je nepravděpodobné že se tam nakopíruje nějaký červ (ty se ukládají do adresářů které jsou tak nějak na všech počítačích) a ty soubory jsou intenzivně využívané.

Také se zde vylučují soubory jako např. c:\pagefile.sys (odkládací soubor windows – swap) a c:\hyberfil.sys (sem se odkládá paměť počítače v případě „režimu spánku“).

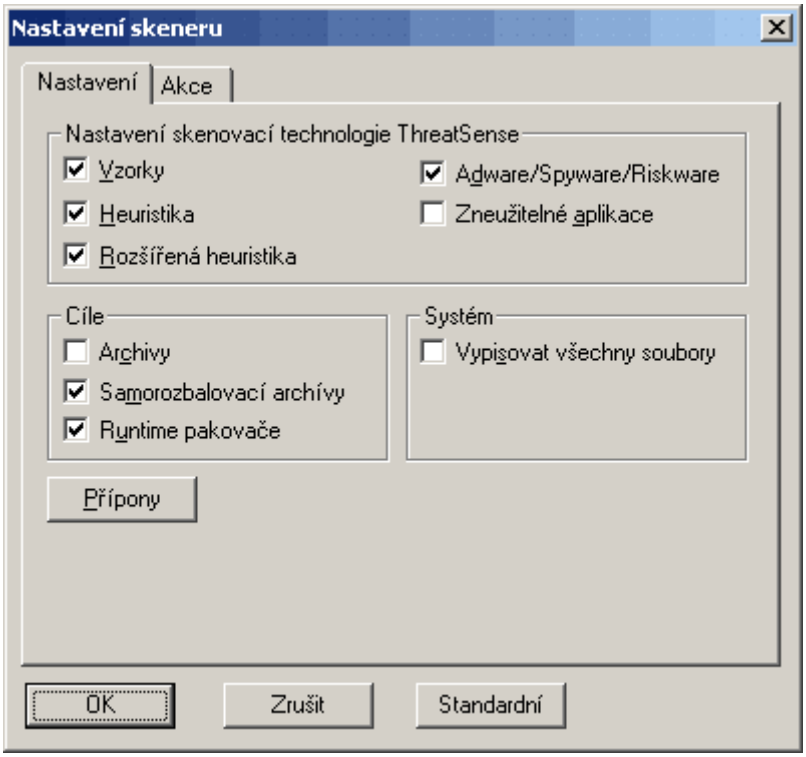
V žádném případě by zde ale neměly být vyloučeny adresáře c:\windows nebo c:\winnt, paušálně celý Program files a kořenový adresář c:\
Prostě: méně je více!



Toto je dodatečné nastavení modulu, vše nechte nastavené takto.

Modul DMON

Tento modul má podobnou funkci jako AMON, jenom se to týká souborů Microsoft Office (verze 2000 a vyšší) a také automaticky stahovaných doplňků Internet Exploreru (verze 5 a vyšší).



Nastavte si to alespoň takto.

Přípony nechte standardní z instalace – tj. testovat všechny soubory.

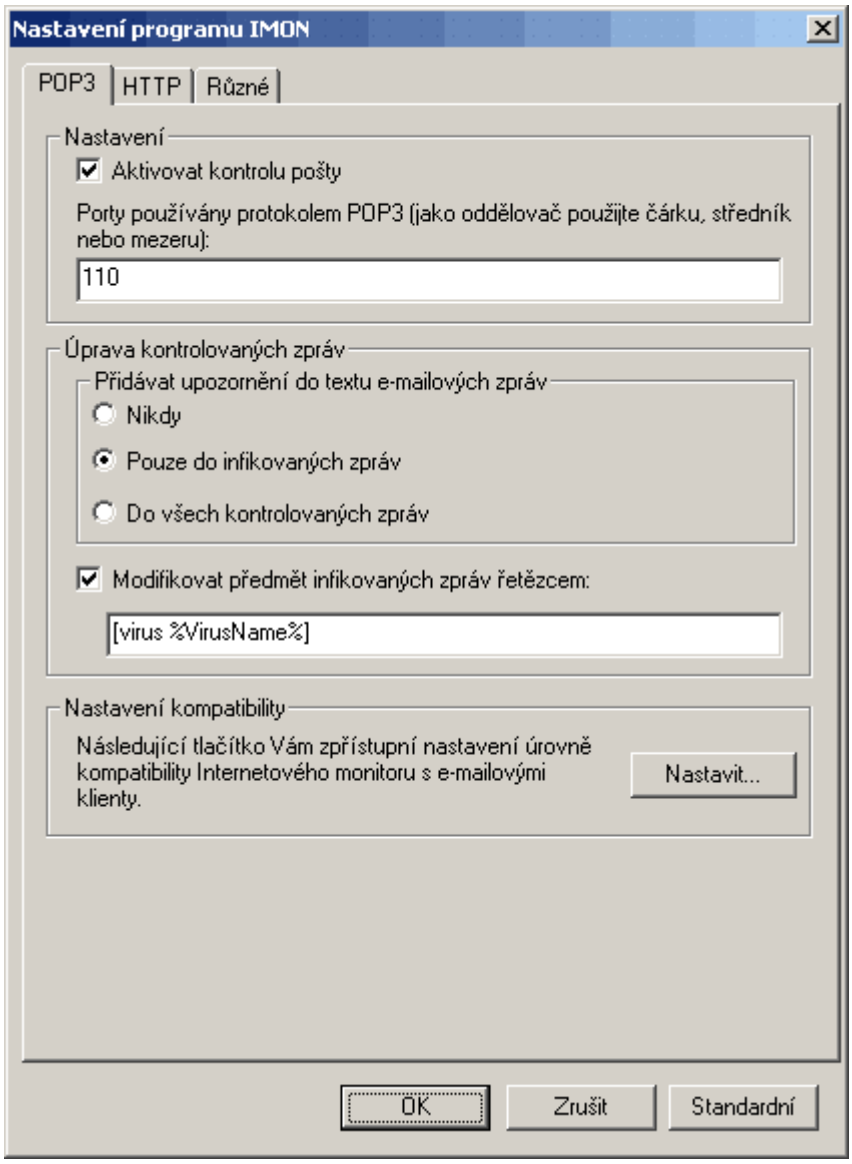
Na záložce nechte také standardní nastavení – pro všechny typy „upozornit/nabídnout akci“.

Modul EMON

Tento modul nechte aktivní pouze v případě, že používáte plného klienta pošty MS Outlook, nebo Exchange. Pro OutlookExpress, Thunderbird apod. se neuplatňuje.
Pokud ho používáte, nastavte ho stejně jako moduly AMON a DMON.

Modul IMON

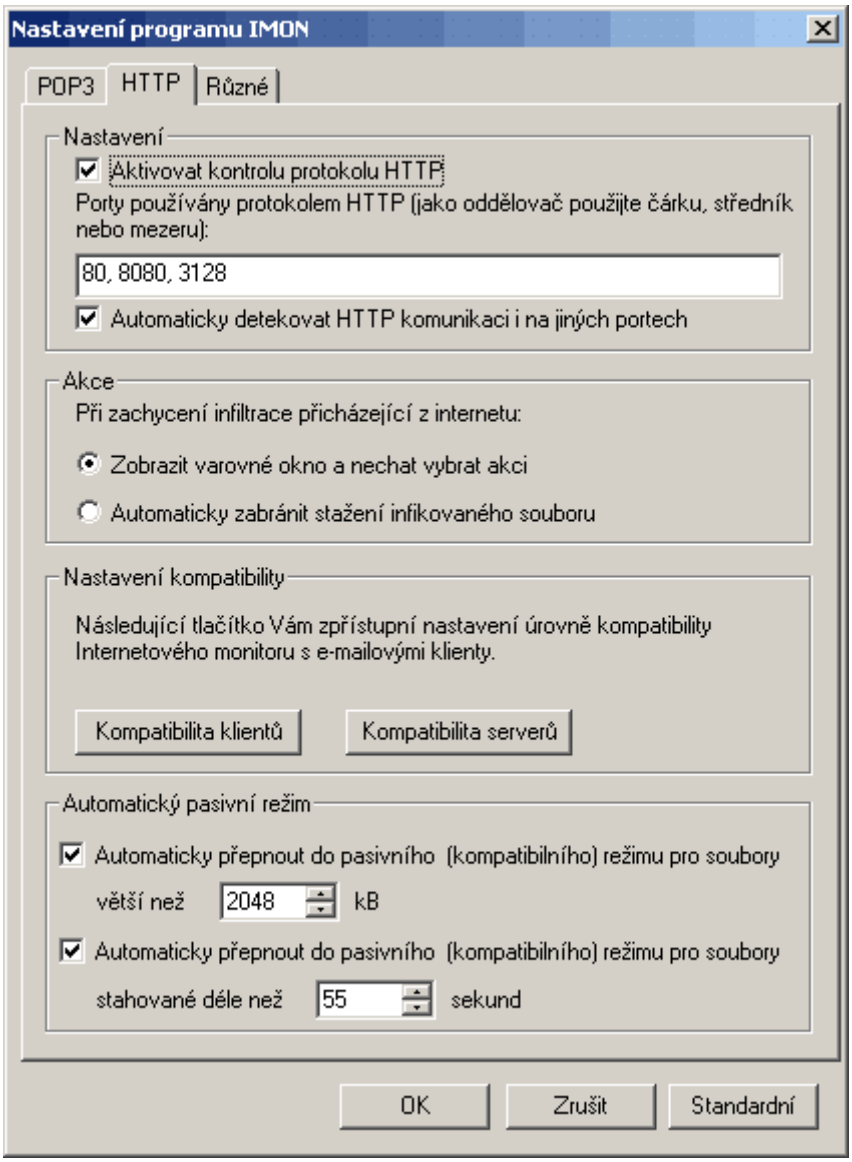
Velice důležitá součást programu. Zajišťuje vlastně stejné funkce jako AMON, ale pro internetový provoz – brouzdání webem, práci s poštou.



POP3 – příjem pošty.

Tady vyhovuje standardní nastavení, jenom je vhodné přidávat upozornění pouze do infikovaných zpráv.

Pod tlačítkem Nastavit najdete nastavení kompatibility s programy – nechte „maximální efektivnost“ – s běžnými programy (OutlookExpress, Thunderbird) to funguje naprosto správně.
Pouze pokud by byl nějaký problém s příjmem pošty, je možné nastavit hejblátko trochu doleva. Ale jenom v nezbytných případech!



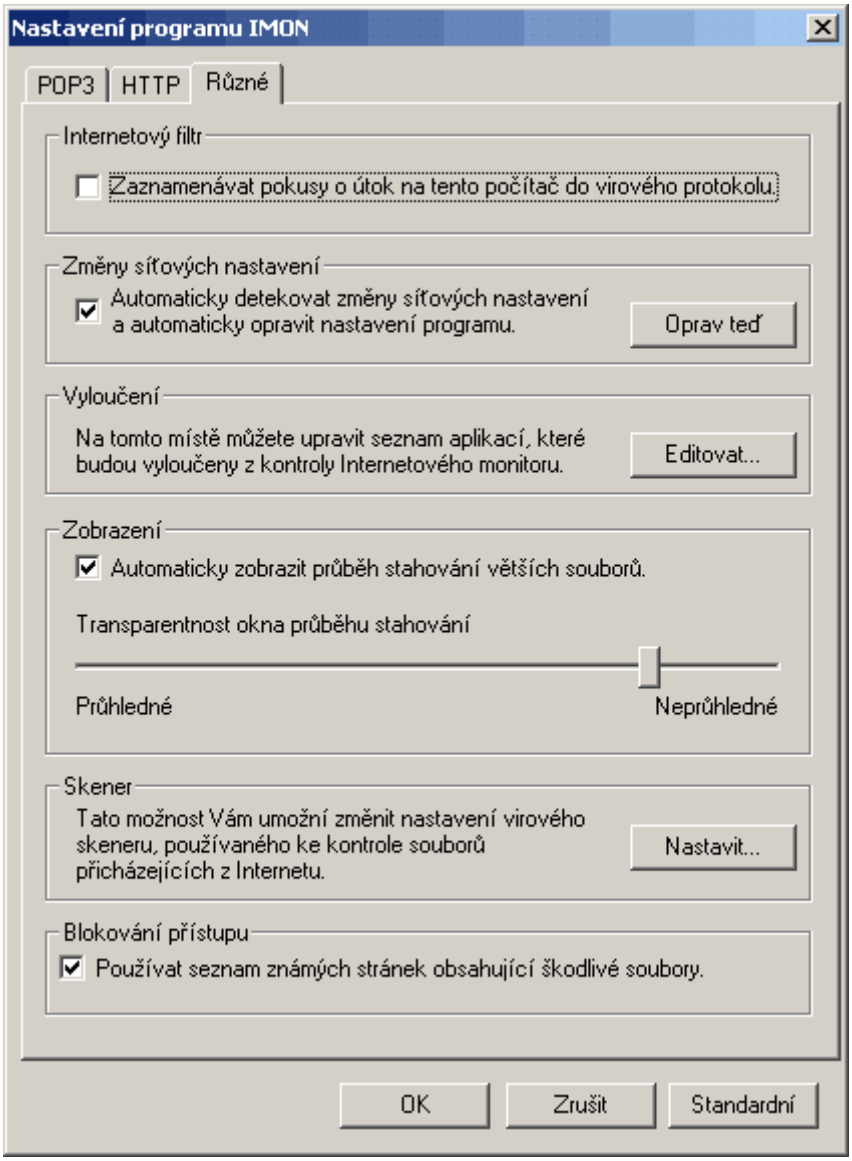
HTTP – internet tak, jak ho všichni vidíme. Prostě web.

Seznam portů – nechte standardně. Stejně je NOD schopný detekovat komunikaci i po jiných. Pouze pokud jste si jisti, že komunikujete hodně s nestandardně nastavenými servery, dopište sem číslo portu.

Akce – laikům a začátečníkům je doporučeno zapnout druhou možnost „automaticky zabránit“.

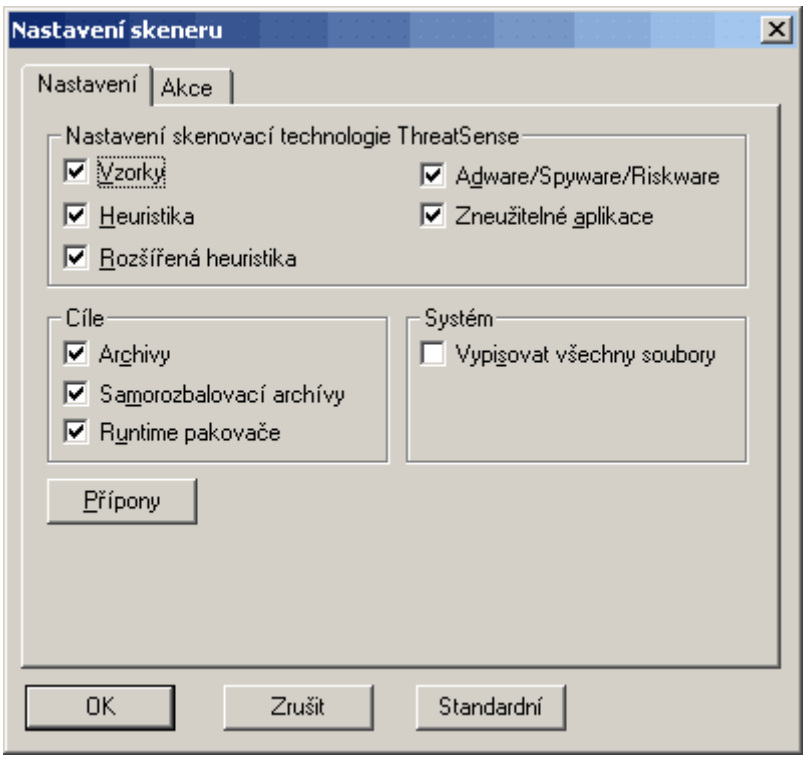
Pod tlačítkem Kompatibilita klientů je vidět seznam programů, které někdy komunikovali tímto protokolem HTTP a NOD je identifikoval. Všechny mají od základu pro jistotu nastavenu vyšší kompatibilitu (slučitelnost). Zde tedy můžete jednotlivým programům zapínat „vyšší efektivnost“ a sledovat jestli fungují stále správně. Pokud ano, tak je samozřejmě vyšší efektivnost lepší. Standardní nastavení ale naštěstí vyhovuje také.

Kompatibilita serverů – to samé, co pro klienty, lze serverům určit režim kontroly bez ohledu na program, kterým tam lezeme. Např. porno servery bych bez začervenání ihned zařadil do režimu vyšší efektivnosti.



Zde nechte standardní nastavení.

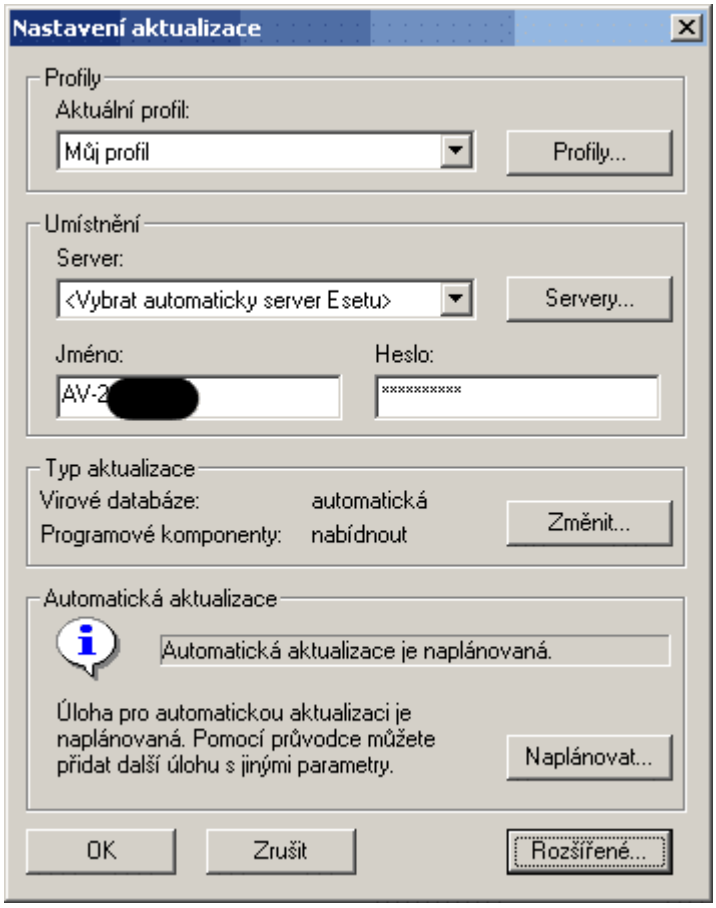
Lze tu také nastavit programy, které budou naprosto vynechány (vyloučeny) z kontroly tímto modulem. Doporučeno je nevyplňovat nic. Mohou se ovšem naskytnout programy, kterým NOD bude prostě vadit. Sice o žádném nevíme, ale umíme si ho představit – např. specializované bankovní programy, multimédia apod.



Zde platí vše, co bylo řečeno u modulů AMON a DMON. Doporučeno je zaškrtnout vše, tak jako na obrázku.

V příponách opět „testovat vše“.

Aktualizace programu

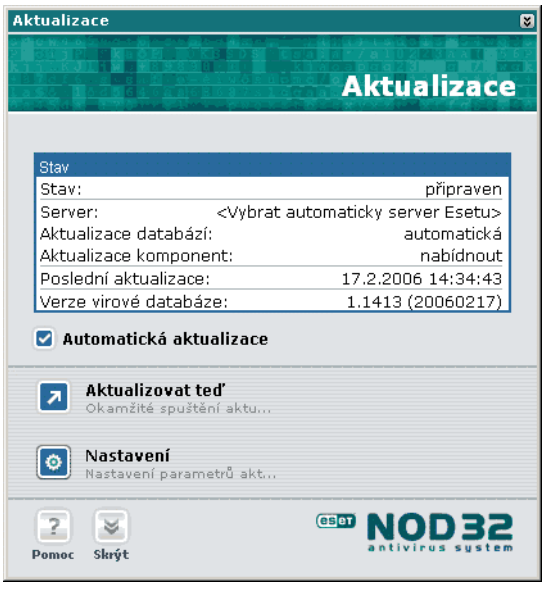


Zde je naprosto nutné nastavit jméno a heslo pro aktualizace – obdrželi jste ho po zaplacení od společnosti Eset a po uplynutí zaplacené doby se musí změnit!!! A logicky znovu zaplatit …

Typ aktualizace je možno nechat tak, jak je na obrázku, ovšem je potřeba vždy odsouhlasit aktualizaci programových komponent (dá to na vědomí poměrně velkým okénkem) když je potřeba (nestává se to často). Změnit to lze stejnojmenným čudlíkem. Je tam také k nalezení reakce na restart počítače – doporučeno je „v případě potřeby nabídnout restart“. Pak by se nemělo stát, že se počítač nechává pouze usínat a k restartu nedojde nikdy!

Profily jsou potřeba pouze pro firemní a cestující počítače – např. pokud jsem v kanceláři na firemní síti, tak je aktualizace z firemního serveru (tj. jiný profil) a pokud jsem zrovna na cestách tak z oficiálních serverů esetu.

Vzhledem k tomu, že antivirový program bez aktualizací je něco jako děravý skafandr (vypadá, že je v pořádku, ale při prvním použití vás zabije), je nutné občas kontrolovat, zda aktualizace probíhají správně. Každá antivirová firma vydává aktualizace trochu jinak, ale v případě NODu by se nemělo stát, že bude několik dní bez aktualizace. Verzi virové databáze (a její datum) lze zjistit najetím na ikonku NODu vedle hodin počítače, nebo v tomto přehledovém okně.
Je-li tedy verze databáze dost stará, je vhodné zde vyvolat okamžitou aktualizaci a po nějaké době zkontrolovat (zde a pak v „protokolech“).



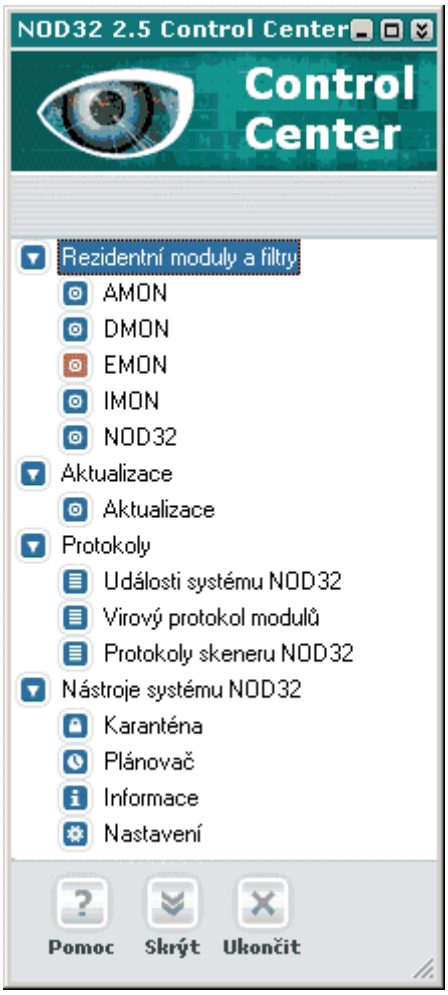
Plánovač.

Zde lze naplánovat nějaké pravidelné akce. Především aktualizace programu a periodické kontroly. Rozepisovat to nebudu, vhodné je standardní nastavení:
Pravidelná automatická aktualizace (každou hodinu)
Automatická aktualizace při přihlášení uživatele
Kontrola souborů zaváděných při startu (při přihlášení uživatele a po aktualizaci)

Nastavení programu

Zde nejsou (s podivem) nijak zvlášť důležitá nastavení. Prohlédněte si to, ale měnit nic nemusíte.
Zajímavá je záložka Upozornění, kde lze nastavit odesílání poplachů elektronickou poštou, nebo „winpopupem“ (na cílovém počítači musí běžet „kurýrní služba“). Je to vhodné např. pro domácí síť, kdy jeden počítač obsluhuje ten, co tomu nejvíc rozumí … tímto se dozví o každém incidentu na ostatních počítačích.

Takto by mělo vypadat hlavní okno

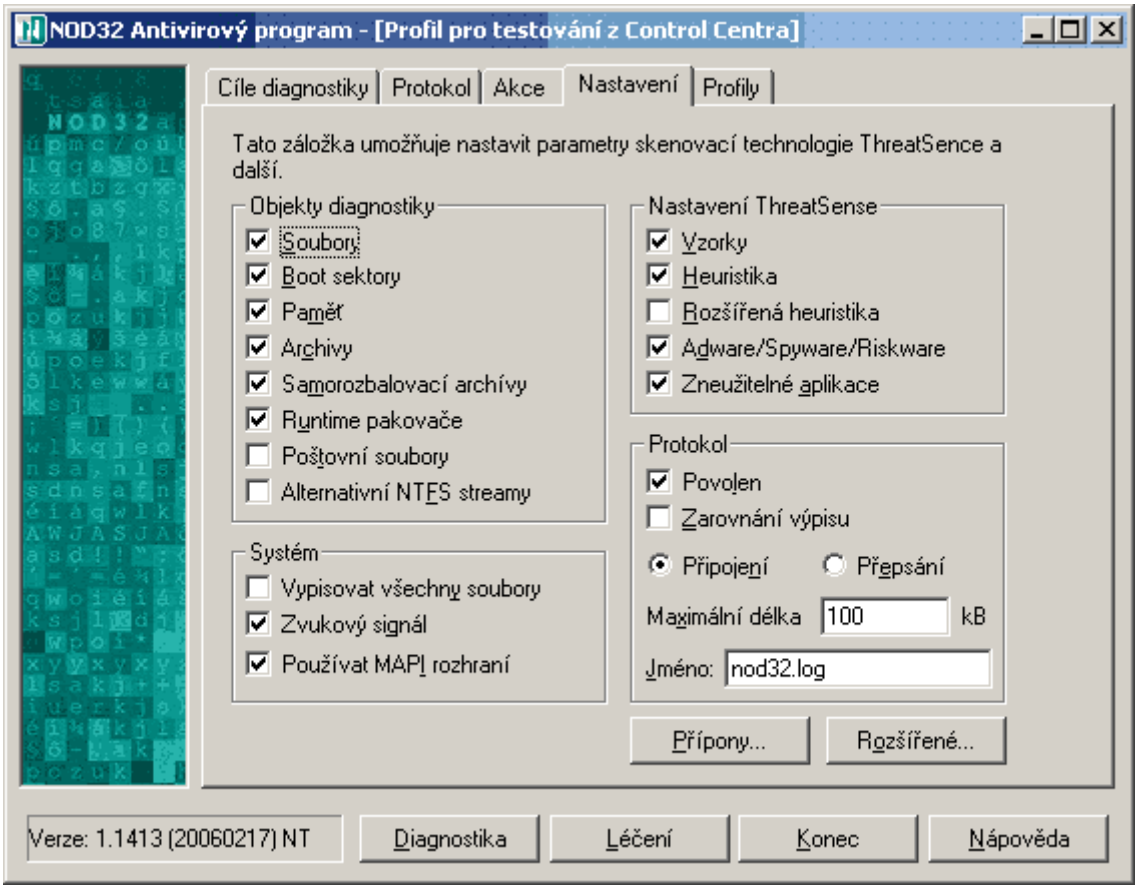


AMON,DMON,IMON aktivní, zbytek může být červený.

NOD32 – vlastní testovací rozhraní.

Toto není modul, ale relativně samostatný program, který na požádání zkontroluje soubory na přítomnost virů. Je vhodné ho spustit jednou po nainstalování a první aktualizaci NODu a potom vždy po instalaci nějakého programu, případně aktualizaci windows. Mezidobí v pohodě zvládne modul IMON.
Pozor, NOD rozlišuje režim diagnostiky a léčení. V tom prvním dá pouze na vědomí, že je v počítači nějaká nákaza, ale neumožní s ní cokoliv ihned udělat!

Napoprvé je dobré ho trochu nastavit. Tj. spustit NOD, přepnout se na záložku profily, jeden si vybrat a na záložce Nastavení nastavit toto:



Poštovní soubory nejsou většinou nutné – v případě se používá standardní klient, který je chráněn modulem IMON.
Alternativní NTFS streamy jsou neviditelné součásti souborů, viry tam můžou mít uloženy některé své části (ne všechny, to by se pak nedokázaly aktivovat).
Rozšířená heuristika – platí pro ni to, co je napsáno u modulu AMON. Automaticky je zapnutá v případě spuštění NODu tlačítkem „hloubková analýza“.

Po nastavení těchto voleb je potřeba stisknout tl. Konec a povolit uložení profilu. Poté udělat to samé se všemi ostatními profily.