STUDIJNÍ MATERIÁL PRO TECHNICKOU CERTIFIKACI
ESET Smart Security, ESET NOD32 Antvirus

Eset software spol. s r.o., Meteor Centre Office Park, Sokolovská 100/94, 180 00 Praha 8
tel.: +420 233 090 233, fax: +420 233 090 230, obchod@eset.cz, www.eset.cz

Obecné vlastnosti produktů ESET

- nenáročný na HW a systémové prostředky
- vyspělý emulátor kódu => rychlá schopnost rozlišení toho, co je z hlediska analýzy důležité a co nikoliv
- minimalizováno množství diskových operací (hlavní „brzda“), využití dynamické cache => prokazatelně nejrychlejší skener na trhu
- další zrychlení: způsob interního třídění signatur, rezidentní modul (opakované přístupy nevedou ke kompletnímu otestování)

ThreatSense® Technology :

skenovací motor všech produktů ESET

Soubor detekčních metod, vrátaně:

Exaktní detekce – **Virové signatury**
- klasická ochrana, vzorky na konkrétní infiltrace

Generická detekce – **Generické signatury**
- vzorky detekující celé rodiny infiltrací

Heuristika – **Analýza kódu**
- pasivní analýza kódu

Rozšířená heuristická analýza – **pokročilá úroveň detekce**
- metoda zajišťující detekci dosud neznámé havěti
- jedna z mála s prokazatelnou úspěšností v současné době

Součástí technologie ThreatSense® i
- generický „unpacker“ - schopný proniknout přes dosud neznámé interní komprese (popř. varianty známých)
- modul pro dekompresi interních kompresních algoritmů i klasických archivních formátů (.RAR, .ZIP...). Schopnost rozbalování zaheslovaných archivů (.ZIP).

ThreatSense® se aktualizuje i v rámci běžné virové aktualizace.

Technologie Antistealth

- vylepšuje detekci rootkitů

- on-demand scanner a kontrola souborů spouštěných po startu „vidí“ skutečný stav, ne falešný, prezentovaný rootkitem
- uživatel nemusí mít žádné znalosti o rootkitech

Technologie ThreatSense.Net

- navazuje na ThreatSense®
- systém zasílání podezřelých souborů k analýze (systém hashování – pošle se jen to, co „ještě nemáme“)
- zasílání statistických informací
- službu využívá okolo 20 miliónů uživatelů
- výsledky nejsou prozatím veřejné => využíváno především pro zajištění detekce dosud neznámé havěti

ESET Smart Security

Instalace

Distribuce v .msi balíčkách.
Existuje řada parametrů, kterými lze průběh instalace ovlivnit. Tyto parametry lze použít během přímé instalace i v případě vzdálené instalace. (Pak jsou tyto parametry určeny předem během tvorby instalačních balíčků a během instalace jsou na stanici vnuceny automaticky.)

- /qn

Tichý režim instalace bez zobrazení dialogových oken.

- /qb!

Uživatel nemá možnost instalaci ovlivnit, avšak její průběh je znázorněn "progressbarem" (stav instalace v %).

- REBOOT="ReallySuppress"

Zakáže restart PC po dokončení instalace.

- REBOOT="Force"

Vynutí restart PC po dokončení instalace.

- REBOOTPROMPT =""

Na provedení restartu po dokončení instalace se dotáže (nemůže být použito dohromady s /qn).

- ADMINCFG=”cesta_k_xml_souboru”

Při instalaci bude použito XML nastavení řešení ESET z definovaného souboru.

Instalace s předdefinovanou konfigurací:
Do adresáře se staženým MSI balíčkem dokopírujeme XML konfiguraci z konfiguračního editoru ESET pod názvem *cfg.xml*. Při zahájení instalace (spuštění MSI balíčku) bude automaticky převzato nastavení z *cfg.xml*.
V případě, že by se konfigurační XML jmenoval odlišně, popř. byl umístěn v jiné složce, lze použít parametr *ADMINCFG=”cesta_k_xml_souboru”.*

Procesy v paměti

Po instalaci běží procesy:

- ekrn.exe – jádro programu, zabezpečuje jeho chod a také např. aktualizaci, on-demand skenování
- egui.exe – grafická nadstavba, ovládací rozhraní

Ovládací rozhraní

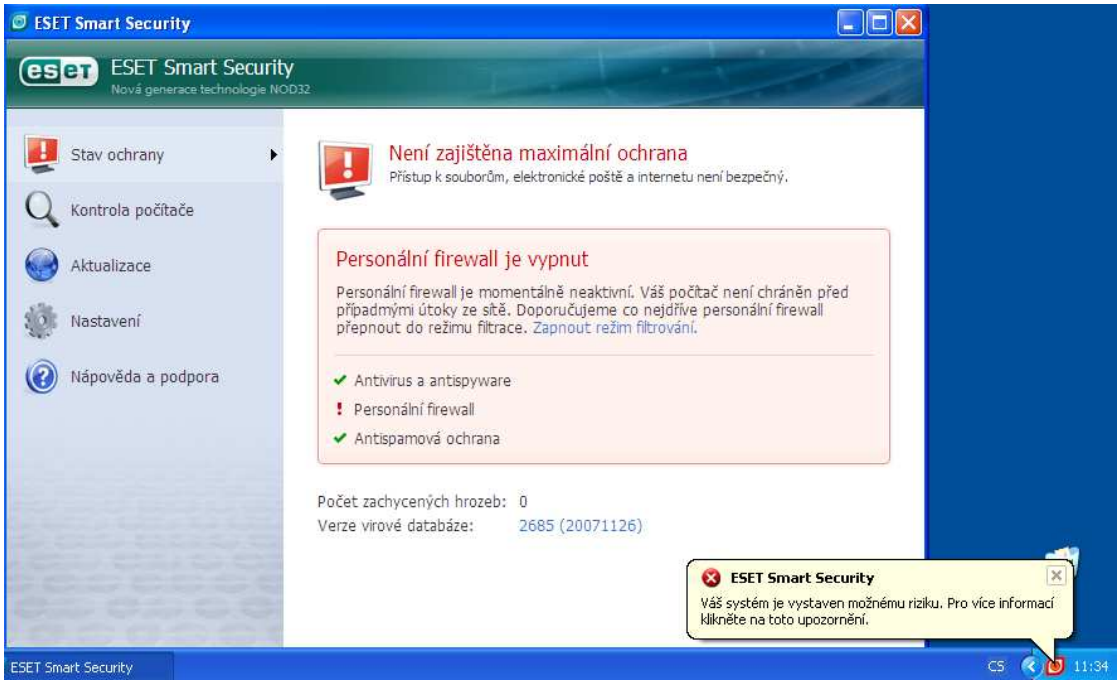
Uživatelský komfort při zachování širokých možností nastavení - dva režimy uživatelského rozhraní:

- **Jednoduchý** – základní nastavení
- **Rozšířený** – pro pokročilé uživatele

Centrální řešení hlavních problémů v menu **STAV OCHRANY** /chyby spouštění modulu ochrany, nefunkční aktualizace/

V případě problémů, nebo neodborného zásahu uživatele ikona stavu ochrany a také ikona v system tray změní barvu, zobrazí se bublinová nápověda a program nabídne řešení:

- červená – zásadní problém
- oranžová – menší problém



Antivirus + Antispyware

Více „samostatný“ („cleaner“ modul). Tři úrovně léčení:

- **Neléčit** – žádná akce. V případě on-demand skenu “Kontrola počítače” se jenom vytváří protokol o infiltracích.
- **Střední úroveň** – ponechává infikované archivy, ostatní léčí/maže
- **Striktní léčení** – maže/léčí infiltrace, maže infikované archivy

Zadané **Výjimky** na soubory/adresáře – platí pro rezidentní modul i pro on-demand scanner Kontrola počítače!

Komponenty:

1. **Rezidentní ochrana souborů a sektorů**

2. **Ochrana pošty**
   - na úrovni poštovních klientů MS Outlook, Outlook Express, Windows mail
   - na úrovni protokolu POP3 (jen kontrola příchozí pošty)

Možnost přidávat upozornění do zpráv a textovou šablonu do předmětu infikovaných správ.

3. **Ochrana přístupu na Internet – HTTP obecně**

!	***Aplikace má problémy při komunikaci s Internetem***
1.	Odznačte ji v seznamu Nastavení (F5) – Ochrana přístupu na web – HTTP - Prohlížeče

Kontrola počítače – on-demand scan

Automatické léčení – přednastavené
Vlastní kontrola – možnost vytváření profilů
Možnost přesunu kontroly na pozadí a spuštění dalších kontrol.

Personální firewall

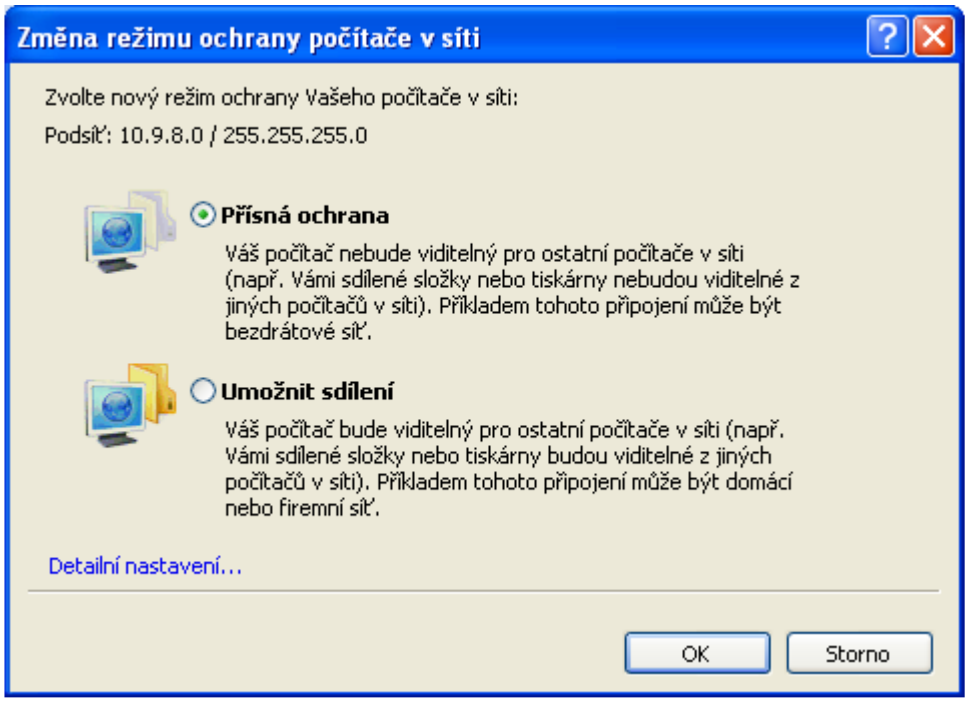
Pokročilý firewall s IDS (Intrusion Detection System) funkcionalitou a s podporou **IPv4** a **IPv6**

- Kontrola různých typů útoků
- Monitorování změn aplikací – pro důvěryhodné aplikace lze nastavit výjimku z monitorování
- Transparentní kontrola HTTP / POP3

Umožňuje definovat tzv. **Důvěryhodné zóny** (Trusted zones) – standardně při vstupu do neznámé sítě

- obvykle síť (identifikovaná IP a maskou), které „důvěřuji“ (moje firemní / domácí síť)

Při vstupu do nové sítě se firewall ptá na režim ochrany (režim lze kdykoliv změnit):



Firewall může pracovat v jednom z tří režimů:

Automatický:
Blokována veškerá příchozí komunikace s výjimkou komunikace inicializované zevnitř. Povolena veškerá odchozí komunikace. Není nutný zásah uživatele.

Interaktivní
Komunikace dle definovaných pravidel.
Komunikace k níž neexistuje pravidlo => dotaz uživateli

Administrátorský
Komunikace dle definovaných pravidel.
Komunikace k níž neexistuje pravidlo => automaticky blokována => žádný dotaz uživateli
Vhodné ve velkých sítích – určení pravidel předem správcem

!	***Komunikace je blokována***
1.	V Nastavení (F5) – Personální firewall – IDS a rozšířené nastavení – „Zapisovat všechna zablokovaná spojení do protokolu.

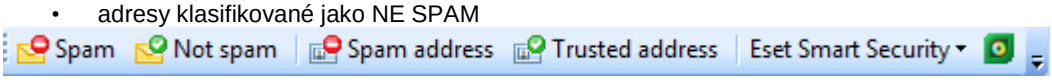
2.	Upravte, respektive zrušte pravidlo.

Antispam

- Automatická filtrace na základě interních pravidel
- Pravidelný update
- Bayesovský filter, seznam důvěryhodných adres Whitelist, seznam spamových adres Blacklist
- Manuální označování spam/not spam, možnost reklasifikace
- Spolupráce s MS Outlook, Outlook Express/Windows Mail

Do seznamu důvěryhodných adres Whitelist se automaticky přidávají:

- adresy z adresáře
- adres příjemců odeslaných zpráv
- adresy klasifikované jako NE SPAM



Spamové správy jsou standardně označeny řetězcem [SPAM] v předmětu správy.

Nástroje

Dostupné v rozšířeném režimu.
Karanténa – skladuje objekty, které nebylo možné léčit v šifrované podobě, je možné je kdykoliv obnovit
Plánovač – úlohy:

- Aktualizace
- Kontrola počítače
- Kontrola souborů zaváděných při startu
- Spuštění externé aplikace

Protokoly -

- Zachycené infiltrace
- Události – systémové události a chyby
- Kontrola počítače – protokol on-demand scanneru
- Protokol personálního firewallu

Další vlastnosti a funkce

- Pokročilé nastavení dostupné z jednoho místa (F5).
- Import/Export nastavení do XML => plně kompatibilní s ERA a konfiguračním editorem ESET
- Technická podpora přímo z programu (automatické zaslání podkladů: protokoly, info o systému...)
- Možnost odesílaní Upozornění a událost (SMTP, Windows Messenger)

Ochrana nastavení heslem – ochrana před změnou parametrů.

!	***Uživatel zapomněl heslo do nastavení, zobrazuje se dialog Potvrzení hesla***
1.	Je potřeba stáhnout aplikaci Unlockv3, vygenerovat ID a zaslat na servis@eset.cz
2.	Počkat si na Unlock code, zadat a kliknout na Unlock.

Klasifikace infiltrací

Existuje několik druhů infiltrací, jejíž názvy jsou obvykle všeobecně známé. Liší se svou povahou a činností. Infiltrace bývají označovány společným názvem **malware**.

VIRUS je program, který připojuje svou kopii ke spustitelným objektům a zabezpečí i její aktivaci. Viry můžeme rozdělovat například podle toho, jaké typy spustitelných objektů napadají. **Souborové viry** napadají spustitelné programy, tj. programy s příponami „exe" a „com". **Boot viry** napadají zaváděcí sektor disku („boot sector", případně „master boot record"), ze kterého se zavádí operační systém. **Makroviry** napadají dokumenty, do kterých je možné vkládat vykonávatelné příkazy (tzv. „makra"), například „doc" a „xls". Další dělení je podle způsobu vykonání škodlivé činnosti. **Viry přímé akce** vykonají svou aktivitu v okamžiku spuštění zavirovaného objektu. **Rezidentní viry** zůstanou v paměti počítače a čekají na vhodnou událost, aby se aktivizovaly. **Retroviry** se pokoušejí znemožnit činnost antivirového programu.

WORM je program se škodlivým kódem, který napadá hostitelský počítač a přes síť se šíří dál. Někdy se tímto pojmem označuje škodlivý program šířící se mailem. Červ se na jiné počítače rozšiřuje aktivněji, kopírováním na lokální síti nebo využitím internetové komunikace (e-mail). Díky rozšířenosti Internetu a poštovních programů se dnes červ dokáže rozšířit doslova po celém světě za několik hodin.

TROJSKÝ KŮŇ je program, který kromě svojí zřejmé funkce obsahuje i škodlivou funkci, o jehož existenci uživatel neví. Častou vedlejší funkcí elektronických trojských koní je umožnit autorovi programu neomezený přístup k počítači s nainstalovaným programem.

Podobnou funkci jako trojský kůň má **BACKDOOR** („zadní vrátka") – aplikace typu klient-server, jehož hlavním úkolem je umožnit autorovi neomezený přístup k počítači. Tyto programy obvykle instalují útočníci z Internetu po úspěšném proniknutí do systému anebo odcházející zaměstnanci.

Fáma (anglicky **HOAX**) není škodlivý kód. Je to druh poplašné zprávy napsané v e-mailu, který ke svému šíření využívá výhradně lidskou důvěřivost. Takovýto e-mail může mít rozličný obsah: dobrou zprávu („kdo tento email pošle dál, vyhraje mobil Nokia"), hrozbu („jestliže tento e-mail nepošlete dál do 48 hodin, postihne vás velké neštěstí), citové vydírání („jestliže tento e-mail dostane milión lidí, velká firma zaplatí transplantaci orgánů chudému dítěti nemocného rakovinou"), důležitou informaci (například varovaní před neexistujícím virem),… Společným prvkem je výzva poslat tento e-mail co nejrychleji všem svým známým.

DIALER je počítačový program, který utváří připojení k Internetu nebo k jiné počítačové síti přes analogový telefon nebo ISDN. V současnosti termín dialer odpovídá hlavně takovému programu, který tuto činnost vykonává bez vědomí uživatele – čímž vzniká uživateli finanční újma.

SPYWARE: program, který odesílá bez vědomí uživatele statistické informace (ty mohou být nejdříve zneužity).

ADWARE je program, který po dobu prohlížení internetových stránek zobrazuje reklamy (obvykle v pop-up oknech).

ROOTKIT je program, který se snaží zamaskovat vlastní přítomnost v PC. Po zabezpečení přístupu do systému může vzdálený útočník nepozorovaně získat plnou kontrolu nad systémem.

Výzkumem počítačových infiltrací s účelem zesílit obranu vůči útokům se zabývá společnost **EICAR** (European Institute for Computer Antivirus Research). Organizace vznikla v roku 1990. Jejím cílem je taktéž napomáhat rychlejšímu rozvoji antivirového softwaru.

Organizace je známá hlavně díky testovacímu souboru se stejným názvem Eicar. Je to spustitelný řetězec, kterým se testuje funkčnost antivirových systémů. Soubor sám o sobě neobsahuje škodlivý kód.