Univerzita Hradec Králové

Fakulta informatiky a managementu

Komparativní analýza řešení HIPS

Bakalářská práce

Autor: Jonáš Horáček

Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové květen 2019

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury či zdrojů.

Podpis:

V Hradci Králové dne 26. 4. 2019 Jonáš Horáček

Poděkování:

Děkuji svému vedoucímu bakalářské práce, panu Mgr. Josefu Horálkovi, Ph.D., za poskytnuté konzultace, které mi pomohly s postupem k vypracování bakalářské práce.

Anotace

Cílem této bakalářské práce je zpracovat problematiku HIPS z pohledu výkonové analýzy na volně dostupná řešení. V teoretické části se představí principy systémů detekce průniku (IDS) a systémů prevence průniku (IPS), dále jejich typické rozdělení na WIDPS, NBA, NIDPS a hlavně HIDPS. V praktické části bude provedena komparativní analýza vybraných volně dostupných řešení. V rámci analýzy budou zohledněny nároky řešení HIPS na systémové zdroje a následně případné ekonomické dopady jeho implementace v prostředí podniku.

Annotation

Title: Comparative analysis of HIPS solution

The mason of this bachelor thesis is to formulate problematics HIPS in terms of performance analysis on free available solution. The theoretic part presents principles intrusion detection systems (IDS) and intrusion prevention systems (IPS) and thein typice distribution to WIDPS, NBA, NIDPS and mainly HIDPS. In practical part will be shown komparative analysis selected free available solutions. In the analysis will be considered claims for solution HIPS on systém sources and eventually economic impal simple mentation in business environment.

Obsah

1 Úvod

Počítačová síť je jeden velký svět, bez kterého se v dnešní době neobejde téměř nikdo. Vzhledem k situaci, že se jedná o tak rozsáhlé a nezbytné odvětví, je nutné udržovat patřičnou bezpečnost. Vzhledem ke zvyšujícímu se množství internetových útoků a hrozeb by se počítačová síť, bez dodatečných opatření, stala jejich snadným cílem a to nelze dopustit.

Nestačí síť chránit pouze antivirovým programem či firewallem, jako tomu je globálně zvykem. Za jistých okolností jsou vhodnými pomocníky systémy detekce průniku (IDS) a systémy prevence průniku (IPS). Hlavním účelem systému prevence průniku (IPS) je rozeznání nevyžádané činnosti a jejího následného odepření před vniknutím do zařízení. Systém detekce průniku (IDS) umožňuje pouze rozeznání případné nevyžádané činnosti, žádným způsobem s určitou činností nijak nemanipuluje. Oba dva systémy v mnoha případech spolupracují s firewallem. Někdy se také používá společný název IDPS, což se v této bakalářské práci často vyskytuje.

IDPS systémy se dále dělí do čtyř kategorií, kterými jsou NIDPS (Network-based intrusion detection prevention system), NBA (Network Behavior Analysis), WIDPS (Wireless intrusion detection prevention system) a HIDPS (Host-based intrusion detection prevention system).

Tato bakalářská práce se zakládá na komparativní analýze v rámci řešení, za pomocí systému HIPS.

HIPS (Host-based Intrusion Prevention System) je druhem systému prevence průniku, který sleduje aktivitu na konkrétním zařízení. Je závislý na konkrétním operačním systému, který se na daném zařízení nachází. HIPS má definovaná pravidla, v rámci kterých omezuje nevyžádaný přístup na konkrétní data. HIPS obvykle rozsáhle protokoluje data, která mají souvislost s detekovanou situací. Tyto data mohou být využity k potvrzení doby platnosti výstrah nebo k vyšetření hrozeb.

Teoretická část bakalářské práce představí obecně IDS a IPS systémy, jejich architekturu a komponenty. Budou rozebrány rozdíly mezi nimi a jejich výhody a nevýhody. Nadále budou rozebrány konkrétní IDPS systémy, tedy NIDPS, WIDPS, NBA a převážně tedy HIDPS, jelikož se bude týkat realizace v praktické části.

Praktická část představí realizaci HIPS (Host-based IPS) systému na konkrétních příkladech více způsoby. Realizace řešení se bude aplikovat na desktopovém operačním systému Windows. V závěru se zohlední, jaké bude mít vybrané řešení ekonomický dopad v rámci licenční politiky na případné pořízení některého z vybraných produktů.

2 Představení principů HIPS

HIPS neboli Host Intrusion Prevention System je technologie, která slouží ke sledování podezřelých aktivit na konkrétním koncovém zařízení. Sledování se provádí analýzou síťových událostí, které se vyskytují na konkrétním elektronickém zařízení. Klíčovým cílem pro využití HIPS technologie je udržet zařízení či síť v dostatečném zabezpečení, nezávisle na konkrétním typu kybernetické hrozby. [40]

HIPS technologie využívá databázi monitorovaných objektů systému, která slouží k identifikaci potencionálního vniknutí do počítačové sítě za pomocí analýzy systémového volání, logů aplikací a úpravou souborového systému. HIPS technologie si u každého objektu pamatuje atributy a vytváří kontrolní součet daného obsahu. Veškeré tyto informace jsou bezpečně ukládány do databáze, pro případ potřeby pozdějšího porovnávání mezi sebou. [39]

HIPS využívá kontroly nad úpravou příslušné oblasti v paměti. Tím udržuje seznam důvěryhodných programů. Pokud některý program překročí možnosti svých oprávnění, tak se HIPS systémem zablokuje, a to na základě vykonávání neoprávněných akcí. [39]

Řešení HIPS chrání koncové zařízení před veškerými útoky, ať už jsou známé či neznámé. Pokud dojde k pokusu o učinění kybernetického útoku ze strany malwaru či hackera, tak HIPS v takovém případě blokuje akci a zašle uživateli upozornění, aby mohl učinit následné rozhodnutí, jak krizovou situaci řešit. [40]

2.1 Základní bezpečnostní schopnosti HIPS

Seznam značí ochranu vůči kybernetickým útokům, které malware může způsobit v případě úspěchu při provedení útoku. Následně jsou vyjmenovány ty nejběžnější malwarové útoky, které HIPS technologie zachytává: [40]

- Kontrola nad jinými programy.
- Instalace zařízení či ovladačů tak, aby dostali prioritu před ostatními programy.
- Prolomení přístupu do paměti elektronického zařízení, k vložení nebezpečného kódu do programu, který z vnějšího pohledu působí důvěryhodně.
- Neodsouhlasené ukončení některého programu, který je právě spuštěný. V mnoha případech to bývá například antivirový software.
- Pokus k přepsání důležitých klíčů v registru.

2.2 Rizika HIPS

HIPS technologie je v mnoha případech efektivně využitelná, jsou s ní však spojená i některá rizika. Takovými riziky jsou například falešně poplachy či špatná volba ze strany uživatele. [40]

Falešný poplach je typ upozornění ze strany HIPS technologie, kdy některý z programů, který je zcela legitimní, provádí podezřelé činnosti, a na základě toho HIPS označí daný program jako malware. Z tohoto důvodu jsou nejlepšími řešeními HIPS taková, která využívají kombinaci behaviorálních a podpisových technik. [41]

Příkladem praktického rizika je například to, že HIPS sleduje klíč registru v operačním systému Windows, kterým je například HKEY_LOCAL_MACHINE, odkud jsou programy spuštěny automaticky při provedení startu operačního systému Windows. Operují zde mimo jiné zcela legitimní programy, které využívají také funkce tohoto klíče. Problém nastává v případě, kdy dojde ke změně obsahu daného klíče, tak uživatel dostane vyskakovací upozornění, které dává na výběr ze dvou možností, kterou je buď potvrzení, nebo blokace. Mnoho uživatelů v takovém případě zvolí možnost potvrzení, vzhledem k situaci, že se obdobné dotazování objevuje při instalaci programů. Takové rozhodnutí může vést k nevědomému odsouhlasení nesprávné akce, kterou HIPS technologie označila jako hrozbu a elektronické zařízení se tak může stát kyberneticky infikovaným. [40]

2.3 Implementace HIPS

Implementace HIPS systému zabere mnoho času a přípravy. Je důležité znát, jak bude navrhnuta a realizována počítačová síť, ve které se bude HIPS aplikovat a jak budou fungovat aplikace, které bude daná počítačová síť využívat. V případě špatného pochopení počítačové sítě se mohou vyskytnout vážné problémy v průběhu implementace HIPS systému. [15]

Většina HIPS systémů jsou řízeny tzv. centralizovanou management konzolou. Při implementaci se konfigurují pravidla a politiky, kde je důležité znát, jaké protokoly budou aplikace v dané síti využívat a skrz jaké porty aplikace komunikují. Je také zapotřebí vědět, jestli je komunikace mezi servery a klienty příchozí, odchozí nebo obojí zároveň. Mělo by se zkontrolovat, jestli vybraný HIPS systém poběží s vlastním antivirovým programem. Pokud ano, mělo by se určit, jestli může vybraný HIPS systém běžet současně s již aplikovaným antivirovým či anti-spyware softwarem. Mnoho HIPS systémů přiděluje jejich vlastní antivirový či anti-spyware software. V takovém případě se velice často stává to, že daný HIPS systém nemůže fungovat souběžně s antivirovým či anti-spyware programem jiného výrobce. [15]

3 Představení systémů detekce a prevence průniku (IDPS)

HIPS (Host based Intrusion Prevention System) má velkou souvislost se systémy detekce průniku (IDS) a systémy prevence průniku (IPS), u kterých se často používá společný název IDPS.

3.1 IDS

IDS (Intrusion Detection System) neboli systém detekce průniku je prostředek, který vyhodnocuje činnosti probíhající v rámci určité počítačové sítě. Tyto činnosti jsou případně detekovány, jestliže se jedná o činnosti nežádoucí.

IDS systémy se ze základu rozdělují na kategorie, jimiž jsou systémy detekce anomálie a signature-based systémy. [2]

Mezi nejznámější IDS systém patří Snort. [20]

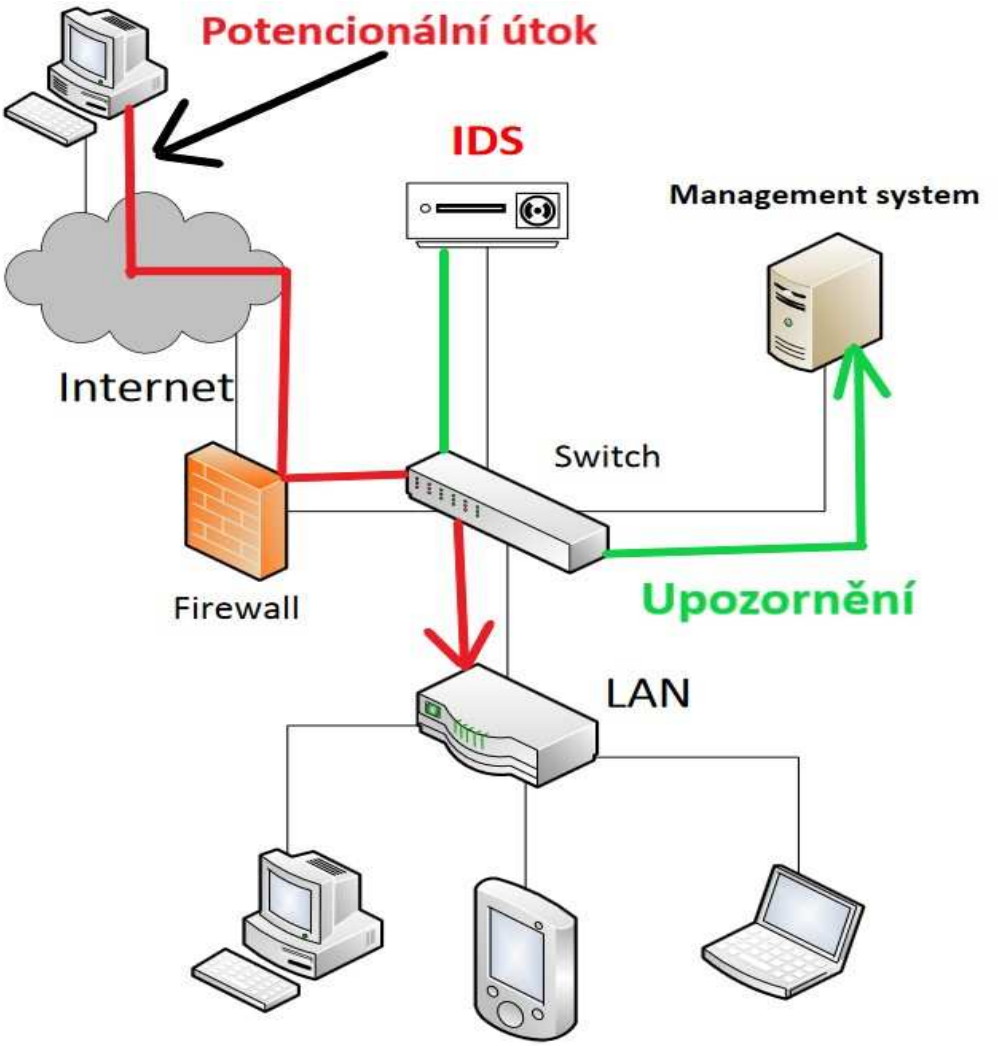
3.1.1 Výhody IDS

Mezi výhody systémů detekce průniku (IDS) zásadně patří realizace prostého rozšíření na celou počítačovou síť a detekce potencionálních útočníků z vnějšího prostředí. Zvládne samozřejmě detekovat i útoky ve vnitřní síti. Stejně jako IPS systémy umožňuje hloubkovou úroveň zabezpečení. Pro systémového administrátora v dané síti je tato technologie prospěšná tím, že poskytuje schopnost určování množství napadení. Další výhodou je možnost uskutečnění centralizované správy korelace případných distribuovaných napadení. [1]

3.1.2 Nevýhody IDS

Jako každý systém má i IDS své nevýhody, mezi které patří například potřeba složitého zprostředkování patřičné odpovědi na každou událost. To je jeden z důvodů, kvůli kterému generují až příliš velké množství dat. Oproti IPS systémům jsou IDS systémy primárně znevýhodněny v případě příchodu potencionálního útoku, kdy na něj pouze reagují, než aby mu nějakým způsobem zabránily před vniknutím. V případě, že se systém setká s dostatečně šifrovaným síťovým procesem, není schopen zpracovat jeho data. Jeho neschopnost také spočívá v tom, že nezvládá sledovat síťovou komunikaci v případě vysoké přenosové rychlosti. Jelikož neumí zcela správně vyhodnotit úplně každou aktivitu, tak se může stát, že občas vytvoří falešné pozitivní zprávy či falešné negativní zprávy. Stejně jako v případě IPS systémů se jedná o nákladnou technologii. [1]

3.1.3 Schéma IDS



Obrázek 1 - Schéma IDS

Přepracováno od zdroje: Kumar - Intrusion Detection System - Types and Prevention

3.2 IPS

IPS (Intrusion Prevention System) neboli systém prevence průniku je prostředek, který dokáže zachytit případnou příchozí nežádoucí aktivitu v síti a kromě pouhé detekce, zvládne také dané aktivitě odepřít přístup.

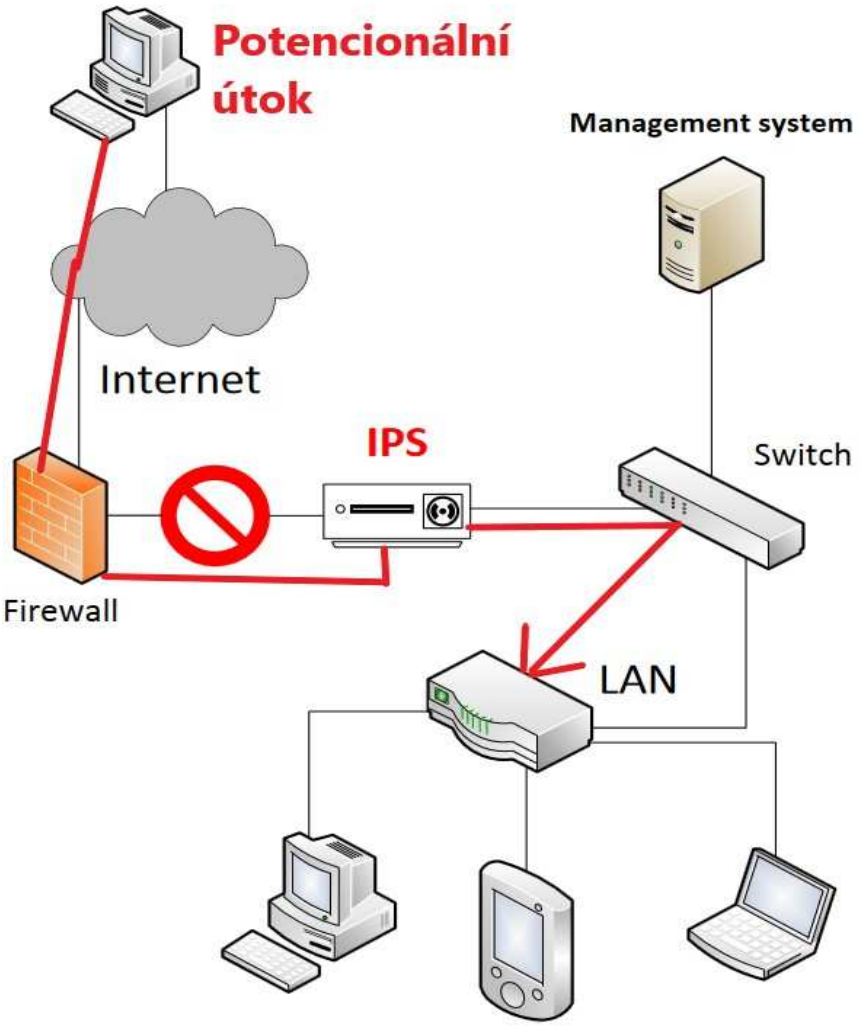
3.2.1 Výhody IPS

Mezi výhody systémů prevence průniku (IPS) zásadně patří realizace korelace události v té chvíli, kdy je to nezbytně nutné. Stejně jako tomu je u IDS systémů, tak i u IPS systémů je k dispozici hloubková úroveň zabezpečení. Tohle je jedna z výhod, kterou se oba typy systémů doplňují. Na rozdíl od IDS systémů, v případě příchodu potencionálního útoku na něj primárně vykonává ochranu, než aby na něj pouze reagoval. Mezi jeho další výhody patří ještě například prospěšná ochrana aplikační vrstvy OSI modelu a možnost behaviorálního přístupu. [1]

3.2.2 Nevýhody IPS

Jako každý systém má i IPS své nevýhody, mezi které patří například to, že vytváří falešné pozitivní zprávy, které mohou v praxi způsobovat problémy. Další nevýhodou je to, že při své funkci vytváří v prostředí dané sítě úzká místa. Jelikož se jedná o zcela přínosnou technologii, tak se ale zároveň stává nákladnou technologií. [1]

3.2.3 Schéma IPS



Obrázek 2 - Schéma IPS

Přepracováno od zdroje: Kumar - Intrusion Detection System - Types and Prevention

3.3 Porovnání IDS a IPS

Jak IDS systémy, tak i IPS systémy mají mnoho společného, tak i přesto jsou mezi nimi určité odlišnosti.

IDS systémy jsou na rozdíl od IPS systémů v počítačové síti těmi pasivními. To znamená, že pokud dojde k detekci nežádoucí aktivity, tak IDS pouze oznámí, že se jedná o nežádoucí aktivitu. Se zjištěnou aktivitou žádným způsobem nepracuje na jejím vyšetření. [1]

Kdežto IPS systémy, kromě detekce nežádoucí aktivity, jsou schopny případ nějakým způsobem vyhodnotit. Nejedná se tedy o pasivní prvky. [1]

Na základě metafory by se mohl uvést příklad na střežené budově, která je vybavena kamerovým snímačem a dostatečným počtem ostražitých hlídačů. V tomto případě kamerový snímač představuje systém detekce průniku (IDS) a ostražitý hlídač představuje systém prevence průniku (IPS). Střežená budova se bere v úvahu jako počítačová síť. Nežádoucí aktivitu by mohla například představovat situace pokusu o loupež. [1]

Pokud nastane pokus o nežádoucí aktivity, vniknutí do určité počítačové sítě, tedy pokus o loupež do střežené budovy, tak kamerový snímač, jakožto systém detekce průniku (IDS) zaznamená aktivitu, ale nikoliv to neznamená její konec, loupež nadále probíhá. Pokud ale zaznamená aktivitu ostražitý hlídač, jakožto systém prevence průniku (IPS), tak loupež ukončí možným zneškodněním pachatele. [1]

3.4 Implementace IDS/IPS

Každý typ IDPS systémů má specifické způsoby k návrhu a implementaci. Z tohoto důvodu by se měl klást důraz na spolehlivost, škálovatelnost, interoperabilitu a zabezpečení.

Spolehlivost

Na základě dosažení spolehlivosti IDPS systému by se mělo zohlednit mnoho faktorů. Jedním z nich je otázka, jestli daný IDPS produkt dokáže pracovat s více než jedním management serverem. V případě, kdy jeden management server dostane výpadek, tak zda automaticky dostanou výpadek i agenti a senzory. Další otázkou je, pokud větší počet senzorů je nasazen ke sledování stejné činnosti, tak v případě, že jeden senzor funkčně selže, zda automaticky přebírá zodpovědnost jiný senzor. Jiným řešením pro případ výpadku jednoho ze senzorů je uzpůsobit konfiguraci k přesměrování na jiný senzor. V rámci spolehlivosti je potřeba také zohlednit, jestli síť neobsahuje redundantní hardware či software. [38]

Škálovatelnost

Na základě škálovatelnosti IDPS systému by se měl klást důraz nejenom na aktuální potřeby společnosti, ale zároveň by se měly nést v úvahu i možné budoucí potřeby. V první řadě je potřeba se zaměřit na dostatečný odhadovaný počet agentů, senzorů, konzolí, management serverů a ostatních komponent IDPS systému. Dále je potřeba zohlednit, jakým způsobem mohou být úložiště v rámci IDPS systémů rozšiřitelné, například pro automatickou archivaci starších dat. Další otázkou je, jakým způsobem více agentů či senzorů zvládne sledovat funkce pro počítačovou síť. Na závěr se musí zohlednit veškeré náklady pro realizaci a potřebné nástroje ke každé možnosti škálovatelnosti.[38]

Interoperabilita

Na základě efektivní interoperability IDPS systému by měla být zaměřena důležitost na to, aby systém zahrnoval zdroje dat, záznam souborů, analýzu záznamu, SIEM software a síťový management software. [38]

Zabezpečení

Na základě efektivního zabezpečení IDPS systému by měl být kladen důraz na zahrnutí ověření, řízení přístupů, auditorské funkce a administrace. IDPS systém by měl být navržen tak, aby byl odolný vůči DoS útokům. Mělo by být zohledněno, jakým způsobem budou ukládána data a jak by měla být chráněná komunikace mezi IDPS komponenty. [38]

4 Architektura

Architektura u systémů detekce či prevence průniku (IDPS) je uspořádaná struktura, která obsahuje veškeré potřebné části či komponenty IDPS ve správném stavu. [1]

Architektura je nejčastěji v optimálním stavu, když každé zařízení, proces a komponenty jsou ve stavu, kdy provádí svoji činnost správnou metodou. Z čehož vychází efektivní vyhodnocení informací a případné odezvy. [1]

V případě, že je architektura špatně uspořádána, mohou se v průběhu procesu vyskytnout nežádoucí jevy. [1]

4.1 Agent

Agent u IDPS systémů je z obecného hlediska něco jako soubor činností, které jsou mezi sebou navzájem nezávislé. Znamená to, že v případě, kdy selže jeden z nich, tak ostatní pokračují stále ve své funkci. Agenti jsou určeni k analýze událostí probíhajících v sítí a ke sledování chování systému. Agenti mezi sebou v průběhu činnosti komunikují za pomoci jednoho protokolu, který je k dané práci určený. V průběhu implementace agenta by mělo být začleněno komunikační rozhraní, odposlouchávač a zasílatel, je to běžné minimum pro uzpůsobení dané věci. Komunikační rozhraní slouží agentovi pro vzájemnou komunikaci mezi ostatními komponenty. Zasílatel je určen k zasílání zpráv dalším komponentům, čímž můžou být například další agenti. Odposlouchávač je určen k příjmu zpráv a dat od senzorů či agentů. [1]

4.2 Senzor

Senzor u IDPS systémů je z obecného hlediska něco jako vstupní prvek v daném systému. Jejich funkce spočívá v tom, že zaznamenají určitá data, která poté předají ke zpracování. Senzory se ze základu dělí na dva typy, a to senzory založené na síti a senzory založené na uzlu. [1]

Senzory založené na síti mohou být buď v provedení softwaru, nebo mohou fungovat jako hardwarové zařízení, která zaznamenávají pakety a jejich data v dané lokální síti (LAN). Z paketů berou hlavně zdrojovou IP adresu, cílovou IP adresu, zdrojový port, cílový port, čas, příznaky a počet přenesených bytů. [1]

Senzory založené na uzlu mají uzpůsobenou konfiguraci tak, aby zaznamenávaly pouze data, která náleží určitému uzlu. Data zprostředkovávají do logovacích souborů. Senzory založené na uzlu jsou spolehlivější v síťové analýze, než senzory založené na síti. To je zapříčiněno tím, že u senzorů založených na uzlu jsou data rozčleněná mezi jednotlivými senzory v konkrétním uzlu. [1]

5 Komponenty

5.1 Management server

Komponenta management server slouží jako centralizované zařízení, která převezme zprávy od senzorů a následně provádí jejích správu. Management server má navrch v tom, že dokáže identifikovat i takové případy, které klasický senzor identifikovat nedokáže. Další předností management serveru je korelace. To je funkce, která je specifická tím, že management server dokáže shromáždit informace z událostí do senzorů, ovládané z jedné IP adresy. [6]

5.2 Database server

Komponenta databázový server (database server) je z obecného hlediska něco jako úložiště získaných informací z událostí od senzorů nebo management serveru. [6]

5.3 Konzole

Komponenta konzole funguje jako program, který realizuje rozhraní pro správu IDPS systémů. Bývá obvykle nasazen na osobní počítače. Konzole slouží například ke správě IDPS systému, konfiguraci a aktualizaci senzorů. [6]

6 HIDPS

HIDPS (Host-based intrusion detection prevention systems) je typem systémů detekce či prevence průniku, který sleduje charakteristiku jediného konkrétního hostitele v dané síti, případně síťové události, které je daný hostitel součástí. Během sledování reaguje na případné nežádoucí příchozí aktivity. [4]

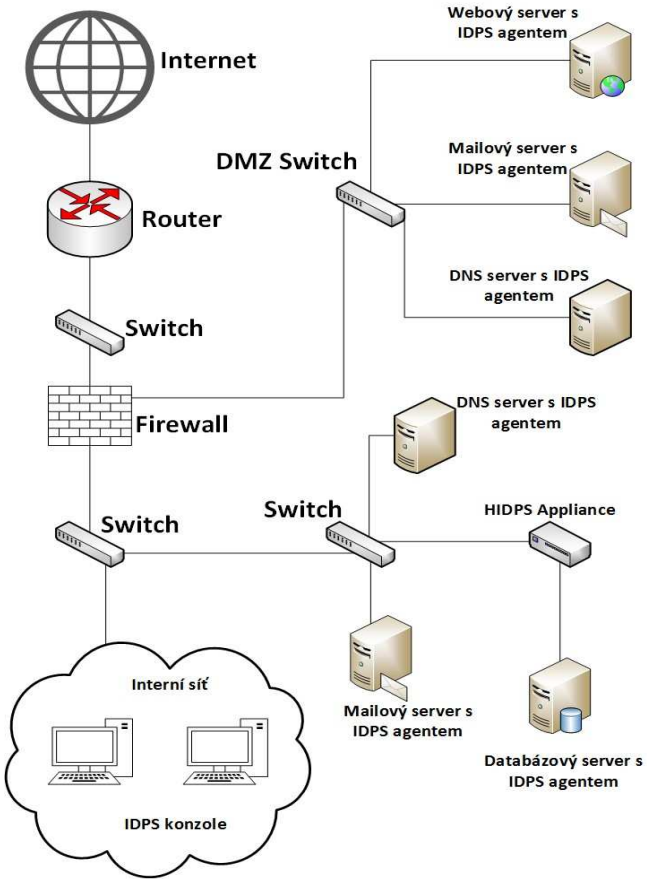
HIDPS systémy jsou nainstalované na konkrétním zařízení, které je sledováno pro případnou potřebu k řešení pokusu o průnik do sítě. Mezi výhody HIDPS patří například schopnost vypořádat se s šifrovaným síťový prostředím a nevyžaduje žádný přídavný hardware. [15]

HIDPS lze rozdělit do čtveřice sub-systémů, které se skládají ze systému sledování souborů, analýzy připojení, log file analýzy a Kernel-based IDPS systému. [8]

6.1 Architektura HIDPS

Architektura HIDPS systémů je svým způsobem jednoduchá. Agenti HIDPS systému jsou uzpůsobeni k funkci u existujícího hostitele v dané síti. Vzájemná komunikace komponentů probíhá v rámci konkrétní sítě, nikoliv za pomoci využití oddělené managementové sítě, jako tomu bývá obdobně u jiných IDPS systémů. V praxi bývají agenti HIDPS systému v mnoha případech uzpůsobeni důležitému hostiteli, kterým může být například server obsahující citlivé informace, které by měly zůstat nepřístupné. [4]

Agenti vysílají data do managementových serverů, které nadále využívají jako úložný prostor pro databázové servery. Pro řízení a obecné sledování jsou určeny konzole. [3]



Obrázek 3 - Architektura HIDPS

Přepracováno od Zdroje: K. Scarfone - Guide to Intrusion Detection and Prevention Systems (IDPS)

6.2 Bezpečnostní schopnosti HIDPS

Mnoho HIPS systémů je schopno uskutečnit detekci pro velké množství typů škodlivých aktivit. Běžně se u nich využívá kombinace typu detekční techniky signature-based, k rozeznání známých případů nežádoucích aktivit a detekční techniky anomaly-based, zahrnující politiky či pravidla k rozeznání neznámých případů nežádoucích aktivit. [4]

6.3 Výhody HIDPS

Mezi silné stránky HIDPS systému patří možnost analýzy činnosti, která je přenesena do šifrované komunikace na základě principu konec-konec (end-to-end). Jedná se o technologii, která nevyžaduje vysoké nároky na technické vybavení pro elektronické zařízení. Umožňuje odepřít přístup potencionálním útokům na úrovni systému. Další výhodou této technologie je schopnost identifikace vniknutí do určitého zařízení. Tato schopnost vychází z aktivity sledování souborového systému, systémového volání, souborového přístupu a síťové události daného zařízení. [8]

6.4 Nevýhody HIDPS

Mezi slabé stránky HIDPS systému patří například možnost sledování síťových útoků pouze na konkrétním zařízení, kde je tato technologie nasazena. V prostředí podniku je nutné ho nainstalovat na každé zařízení zvlášť, ať už se jedná o virtuální zařízení, hypervizor či fyzické zařízení. Generování výstražných upozornění přichází se zpožděním. Další nevýhodou této technologie je případ, který může způsobit špatnou komunikaci mezi jinými bezpečnostními prvky v zařízení. Oproti NIDPS systému je tato technologie znevýhodněna závislostí na konkrétním operačním systému. [8]

6.5 Schopnosti prevence HIDPS

HIDPS systémy disponují schopnostmi pro prevenci průniku. Detekční techniky jsou u každého produktu rozdílné, tudíž jsou schopnosti prevence HIDPS systémů rozděleny, do čtyř kategorií. Mezi schopnosti prevence pro HIDPS systémy patří analýza kódu, analýza síťového provozu, filtrování síťového provozu a sledování souborového systému. Existují i jiné detekční techniky HIDPS systémů, které ale neumožňují prevenční činnosti, protože veškeré události jsou identifikovány, až po jejich uskutečnění. Mezi tyto detekční techniky patří sledování konfigurace sítě, analýza logů, kontrola integrity souborů či atributů. [3]

Analýza kódu

Techniky analýzy kódu mohou odepřít spuštění kódu, včetně malwaru a nevyžádaných aplikací. Některé HIDPS systémy umožňují zastavení síťových aplikací, před zahájením shellů, které by mohly být zneužity k jistým síťovým útokům. V případě správné konfigurace je tento typ detekční techniky značně efektivní, při zastavení neznámých útoků. [3]

Filtrování síťového provozu

Filtrování síťového provozu je typ detekční techniky, který pracuje jako Host-based firewall. Jeho schopnost spočívá v možnosti zastavení nevyžádaného přístupu a pokusu o porušení zásad bezpečnostní politiky, která může být způsobena například použitím nevhodné externí služby. Efektivita této techniky nabývá pouze v případě zastavení nevyžádané aktivity, která je identifikovaná, na základě IP adresy, UDP portu, TCP portu či ICMP protokolu. [3]

Analýza síťového provozu

Analýza síťového provozu umožňuje zastavit vstupní síťový provoz, před vyhodnocením určitého hostitele a výstupní síťový provoz, před odesláním od hostitele. Tato činnost nabývá užitku při zastavení útoků na síťovou, aplikační a transportní vrstvu referenčního modelu ISO/OSI. Užitku nabývá také i při zastavení používání nepovolených aplikací či protokolů. Analýza umožňuje také rozeznat stažené či přenesené škodlivé soubory pro dané zařízení a následně jim znemožnit uložení. Tento typ detekční techniky je nejvíce účinný pro zastavení pro mnoho známých a dříve neznámých síťových útoků. [3]

Sledování souborového systému

Sledování souborového systému umožňuje ochranu souborů před přístupy, přemístěním, odstraněním a modifikací. Tato ochrana je užitečná k odepření přístupu k instalaci malwaru, rootkitů, trojských koní a dalších útoků, které jsou určeny, k nevyžádanému přístupu k souborům. Tento typ detekční techniky umožňuje poskytnout k dispozici další vrstvu pro řízení přístupu, která funguje jako komplement k existujícímu řízení přístupu na daném hostiteli. [3]

6.6 Omezení HIDPS

HIDPS systémy disponují, jako každý jiný systém i svými omezeními, které je nutné respektovat. Mezi ta nejdůležitější omezení patří prodleva při generování výstrah, centrální prodlevy při odesílání hlášení, problémy při komunikaci s existujícími bezpečnostními prvky, omezení výkonu pro zařízení, na kterém je HIDPS systém nasazen a jejich případný restart. [4]

Prodleva při generování výstrah

Ve většině případů agenti HIDPS systémů generují bezpečnostní výstrahy v reálném čase, v průběhu činnosti určité techniky. Existují i techniky, které se opakovaně využívají k rozeznání událostí, které byly už někdy v minulosti provedeny. Aplikování těchto technik je možné realizovat pouze v omezených časových úsecích, to se následně odráží na prodlevách při generování bezpečnostních výstrah. [3]

Centrální prodlevy při odeslání hlášení

Mnoho HIDPS systémů předává data ohledně výstrah do management serverů, v pravidelných časových úsecích, nikoliv v reálném čase. Data týkající se bezpečnostních výstrah se obvykle přenášejí po částech v úsecích 15 minut až 1 hodina. Menší implementace HIDPS systémů umožňuje přenášet taková data rychleji. Pro větší implementace HIDPS systémů jsou doporučeny přenosy, které nejsou tak časté. V takovém případě může dojít ke zpoždění během odezvy. [3]

Problémy při komunikaci s existujícími bezpečnostními prvky

Instalace agenta může způsobit potíže s jinými bezpečnostními prvky na konkrétním zařízení. Ve většině případů se jedná o takové bezpečnostní prvky, které využívají funkce k zachycení aktivity na zařízení hostitele, čímž je například firewall nebo VPN klient. [3]

Omezení výkonu pro koncové zařízení

HIDPS systémy se od ostatních IDPS systémů liší tím, že zahrnují spuštěné agenty na sledovaných zařízeních. Obsažení agenti v síti mohou mít vliv na zátěž pro zařízení hostitele a to zejména na procesor, operační paměť a úložné místo na disku. Činnosti prováděné agenty mohou mít vliv na zpomalení chodu sítě a využití souborového systému. [3]

Restart koncového zařízení

U mnoho HIDPS systémů může dojít k situaci, že některé změny konfigurace týkající se agenta či aktualizace jeho softwaru mohou vyžadovat restart pro sledované zařízení. V takovém případě se může stát, že agenti nemohou detekovat nejnovější typ síťové hrozby, protože například důležité koncové zařízení nemohlo být restartováno. [3]

6.7 Implementace HIDPS

K implementaci konkrétního HIDPS systému je potřeba navrhnout architekturu, uskutečnit testování komponent HIDPS systému, provést zabezpečení komponentů a následně jejich nasazení. [3]

Pokud se v testovacím prostředí posoudí komponenty daného HIDPS systému, měl by se ve zrealizovaném prostředí nasadit malý pilotní program, který umožňuje přizpůsobit aktivity a provádět vylepšení.[3]

V případě, že management servery či konzole vyžadují ověření pro každého agenta, aby mohly provádět jejich správu nebo shromažďovat jejich data, je potřeba zajistit pro ověřovací nástroje správu a zabezpečení. [3]

7 NIDPS

Pro komplexní řešení zabezpečení LAN sítě a s tím i jeho koncových stanic je v kontextu práce nutné představit i řešení NIDPS.

NIDPS (Network-based intrusion detection prevention systems) je typem systému detekce či prevence průniku, který sleduje komunikaci v síti u konkrétních zařízení či síťových celků. Mimo sledování komunikace v sítí zároveň provádí analýzu určité sítě a aplikačních protokolů k rozeznání podezřelé příchozí aktivitě. [3]

V případě, že NIDPS pracuje v promiskuitním režimu na síťové kartě (NIC), může být využit k síťovému odposlechu. Dokonce může zaznamenat i komunikaci v síti, která se netýká přímo daného zařízení. Některé činnosti NIDPS, pracujícího v promiskuitním režimu na síťově kartě (NIC), jsou nezbytně nutné pro udržování správného chodu sítě. [2]

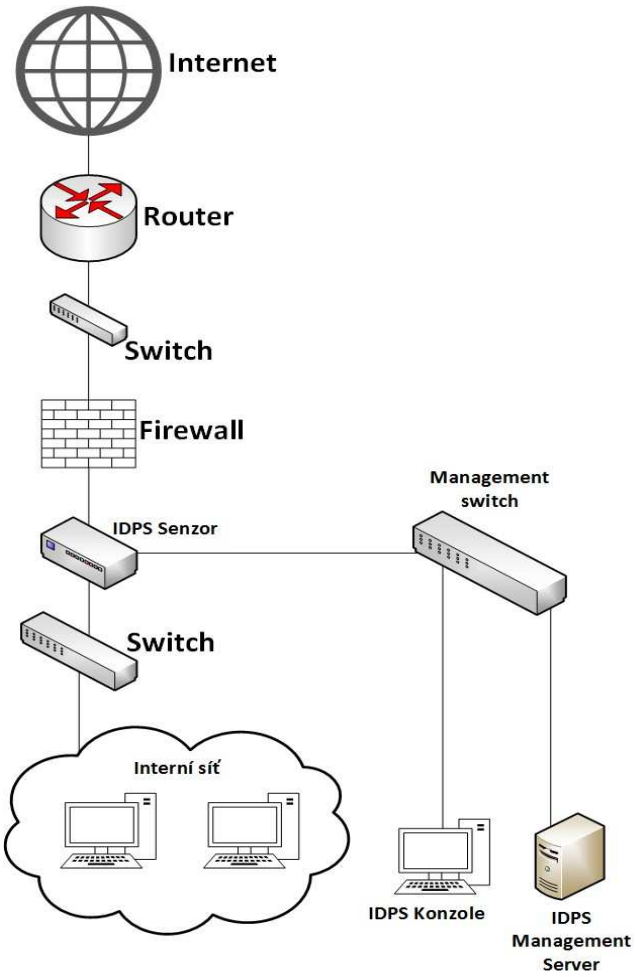
7.1 Architektura NIDPS

NIDPS (Network-based intrusion detection prevention systems) můžou fungovat buď v in-line režimu nebo v pasivním režimu. Existují hybridní inline senzory, které fungují jako firewall a IDPS zároveň. [4]

Inline režim je prakticky realizován tak, že sledovaný síťový proces či komunikace prochází přímo skrz daný senzor. Dobrým důvodem pro fungování inline senzoru je příležitost blokování síťové komunikace za účelem eliminace nežádoucích síťových útoků. [4]

Inline senzory bývají často rozmístěny mezi firewally a síťová zařízení, určená pro správné udržování bezpečnosti sítě. [3]

Pasivní režim je uskutečněn tak, že sleduje aktuální kopii síťového procesu či komunikace. Jinak síťový proces skrz senzor nevstupuje. Pasivní senzory jsou schopny sledovat síťový proces či komunikaci za pomoci různých metod, mezi které patří spanning porty, network tap a IDS loadbalancer. [4]



Obrázek 4 - Architektura NIDPS

Přepracováno od Zdroje: K. Scarfone - Guide to IntrusionDetection and Prevention Systems (IDPS)

7.2 Výhody NIDPS

Mezi silné stránky NIDPS systému patří schopnost analýzy síťového provozu, po celém rozsahu dané sítě. Identifikuje nežádoucí vniknutí sledováním síťového provozu. Zvládá sledovat více počítačových sítí a systémů současně. Umí předejít potencionálnímu síťovému útoku dříve, než daný útok stihne napadnout plánovaný cíl. Na rozdíl od HIDPS systému se jedná o technologii, která je nezávislá na platformě, tudíž je i snadná k nasazení. [8]

7.3 Nevýhody NIDPS

Mezi slabé stránky NIDPS systému patří neschopnost sledování bezdrátových protokolů. Vytváří falešné negativní a pozitivní výroky. Nezvládá detekci síťových útoků u šifrované komunikace a zároveň nedokáže rozeznat šifrované datum. Při vysokém zatížení v síti, není zajištěna plná podpora pro analýzu. V případě přehlcení síťového provozu se může stát, že nebude zpracován každý paket v dané počítačové síti. Velice obtížně pracuje při detekci v prostředí virtuálních sítí. Poslední nevýhodou je nejasné určení ohledně úspěchu síťového útoku. [8]

8 WIDPS

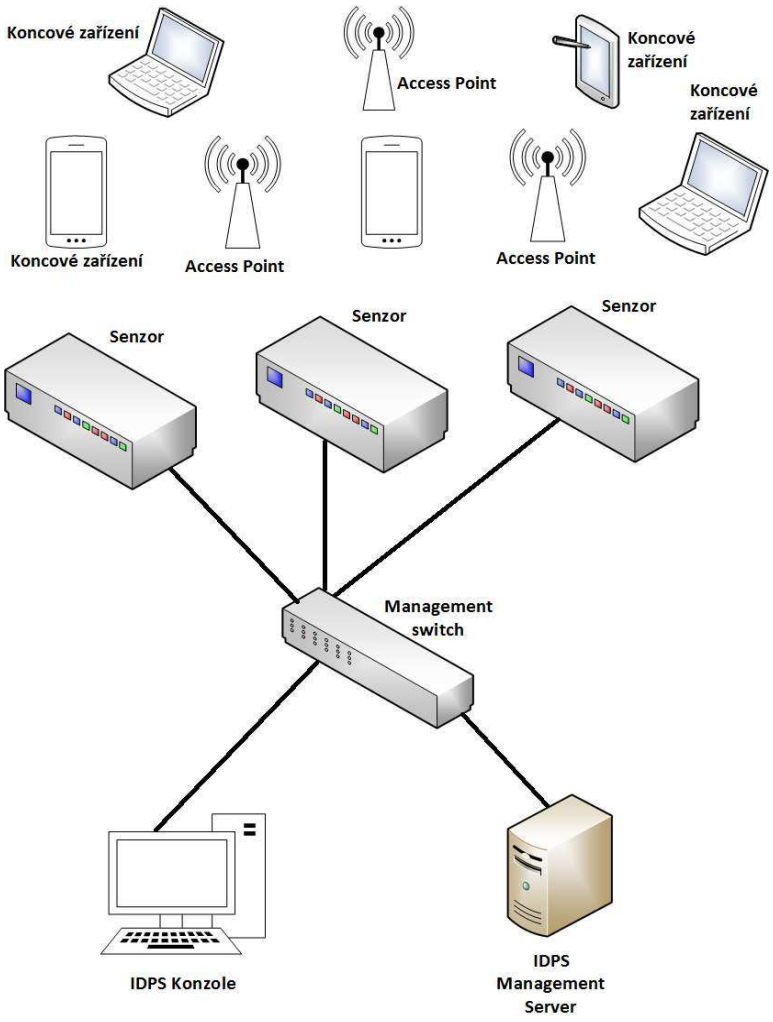
WIDPS (Wireless-based intrusion detection prevention systems) je typem IDPS, který sleduje bezdrátový síťový proces či komunikaci a provádí analýzu bezdrátových síťových protokolů k rozeznání případné nežádoucí aktivity, včetně síťových protokolů samotných. Nejčastějším případem realizace WIDPS systému je uskutečněno v rámci sledování bezdrátové lokální sítě, tedy WLAN. [4]

WIDPS systémy lze využít například k patřičné detekci neobvyklého užívání, DoS útoků, zařízení v bezdrátové síti s nedostatečnou ochranou či neautorizovaných WLAN sítí, případně jejich zařízení. [7]

8.1 Architektura WIDPS

Architektura WIDPS systémů obsahuje stejné komponenty, jako architektura NIDPS systémů. Pouze senzory u WIDPS systémů fungují jinak, než u NIDPS systémů. Jejich funkce se liší právě tím, že se v případě WIDPS systémů se jedná o bezdrátovou komunikaci. [4]

Bezdrátové senzory mohou být dedikované, propojené s access pointem nebo propojené s bezdrátovým switchem. Dedikované senzory se dále dělí na fixní a mobilní. Dedikovaný senzor je komponenta, která pracuje s WIDPS systémem, ale nepřechází síťový proces či komunikaci od zdroje k cíli. Bývá obvykle ve své funkci pasivním senzorem. Bezdrátový senzor propojený s access pointem poskytuje v porovnání s dedikovaným senzorem menší hodnoty zabezpečení, vzhledem k jeho potřebě časové dělitelnosti mezi poskytnutím síťového přístupu a sledováním většího počtu kanálů. Právě z tohoto důvodu je senzor propojený s access pointem vhodnější na případy, kdy je potřeba sledovat pouze jeden kanál či pásmo. Senzory propojené s bezdrátovým switchem existují navzdory tomu, že některé bezdrátové switche mají k dispozici specifické funkce IDPS systémů. Ovšem senzory propojené s bezdrátovým switchem se nemohou ani zdaleka výkonově rovnat senzorům propojených s access pointem či dedikovaným senzorům. [3]



Obrázek 5 - Architektura WIDPS

Přepracováno od Zdroje: K. Scarfone - Guide to IntrusionDetection and Prevention Systems (IDPS)

8.2 Výhody WIDPS

WIDPS systém je jedinou technologii z IDPS systémů, který je schopen analyzovat provoz v rámci bezdrátové sítě za pomocí analýzy činností bezdrátových protokolů a přijetí patřičných opatření. [8]

8.3 Nevýhody WIDPS

Mezi slabé stránky WIDPS systémů patří neschopnost sledovat aktivity protokolů síťové vrstvy, aplikační vrstvy a transportní vrstvy referenčního modelu ISO/OSI. Nezvládá kompenzovat nedůvěryhodné bezdrátové protokoly. Další nevýhodou této technologie je to, že nezvládá se vyhýbat únikovým technikám. [8]

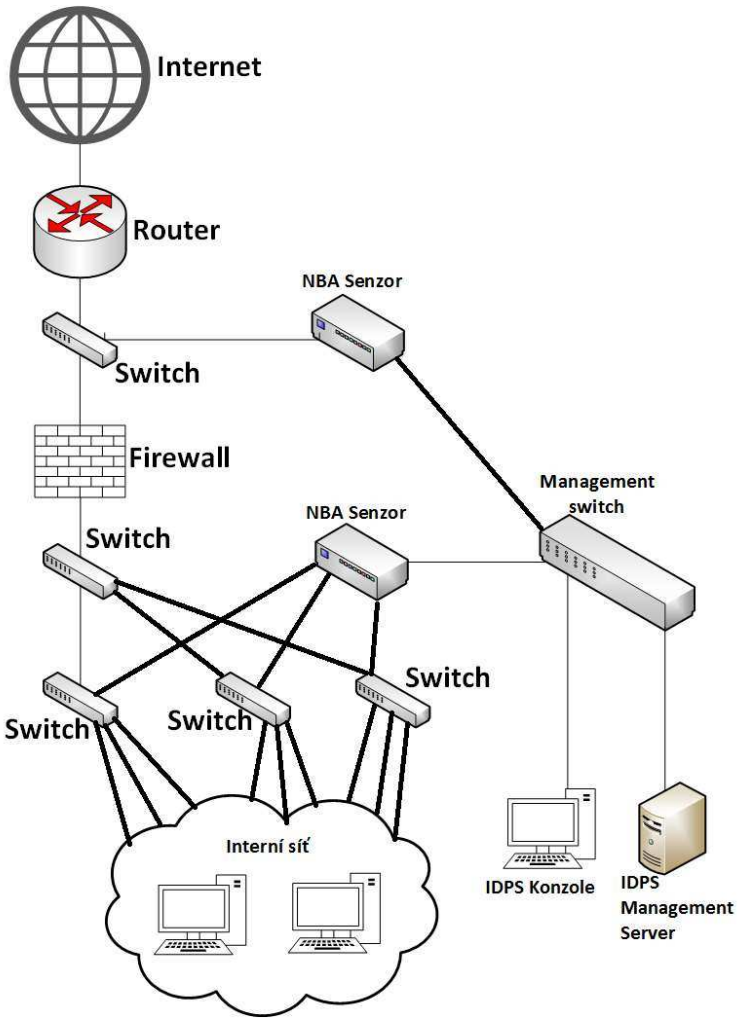
9 NBA

NBA (Network Behavior Analysis) je typem IDPS systémů, který analyzuje síťovou komunikaci či proces nebo její statistické údaje k rozeznání neobvyklého chodu sítě. Většinou neobvyklý chod síť způsobují DDoS útoky, nedodržení zásad bezpečnostních politik a trojské koně. [4]

9.1 Architektura NBA

NBA (Network Behavior Analysis) systémy umožňují běžně senzory, konsole a v některých případech i managementové servery, které v tomto okruhu dostávají i název jako analyzátory. Architektura NBA systémů je uzpůsobena tak, že se u ní odděluje managementová síť pro komunikaci komponentů, stejně jako tomu je u NIDPS systémů. Pokud senzory shromažďují data ze směru toku od jiného zařízení, tak východisko NBA systému může být odděleno od standardní sítě. [3]

Běžný tok dat v síti zahrnuje zdrojovou IP adresu, cílovou IP adresu, zdrojový a cílový port, který se týká protokolů transportní vrstvy TCP a UDP, případně i protokolu síťové vrstvy ICMP. Dále obsahuje také počet směrovaných paketů, počet přenesených bytů a časovou značku. [4]



Obrázek 6 - Architektura NBA

Přepracováno od Zdroje: K. Scarfone - Guide to IntrusionDetection and Prevention Systems (IDPS)

9.2 Výhody NBA

Mezi silné stránky NBA systému patří lepší detekce DoS útoků a rekonstrukce zásadních malware nakažení. Zvládá prověřit síťový provoz k rozpoznání potencionálních hrozeb, které vytváří nadměrný tok, jedná se například o DDoS útoky. [8]

9.3 Nevýhody NBA

Mezi slabé stránky NBA systému patří zpoždění v detekci útoků, jelikož tok dat je přenášen ve skupinách. [8]

10 Analýza dostupných řešení HIPS

Na základě provedení výkonové a funkční komparativní analýzy byla vybrána tři dostupná řešení pro systém HIPS, a to Comodo Internet Security Pro, ReHIPS a DeepSecurity. Na trhu existuje mnoho produktů disponujících technologií HIPS. Tato řešení byla vybrána na základě odlišnosti implementace, realizace, praktického využití, instalace a cenové dostupnosti. Comodo Internet Security Pro je mezi vybranými řešeními antivirový software, který má přidanou hodnotu využití HIPS technologie. ReHIPS je triviální program, který funguje jako samostatný HIPS a není k němu potřeba nějaká větší odborná znalost. DeepSecurity od firmy Trend Micro je z vybraných řešení nejrozsáhlejší pro využití HIPS technologie, u kterého je potřeba znát více, než pouze uživatelské znalosti. Zvolená řešení byla uskutečněna na testovacím zařízení, na kterém se následně provedla výkonová analýza u každého řešení za pomoci nástroje System Explorer. Výsledky výkonové analýzy byly finálně porovnány mezi všemi HIPS řešeními.

10.1 Stanovení výchozích hypotéz

Pro vyhodnocení v rámci technického porovnání vybraných HIPS řešení se stanovily hypotézy, které byly zjišťovány v průběhu analýzy, instalace a sledování výkonu. Stanovilo se průměrné vytížení procesoru (CPU), průměrné vytížení operační paměti (RAM), průměrné vytížení swapovacího oddílu (SWP), hodnota kapacity instalačního balíku, hodnota kapacity programu po instalaci a průměrná doba instalace na daném testovacím elektronickém zařízení. Na základě zjištěných hodnot se provedlo porovnání mezi třemi zvolenými produkty, které se vztahovalo ke komparativní analýze. Komparativní analýza se odvíjí jak ze subjektivního hodnocení při práci s programy během analýzy, tak i z těchto zjištěných hypotéz.

10.2 Specifikace testovacího zařízení

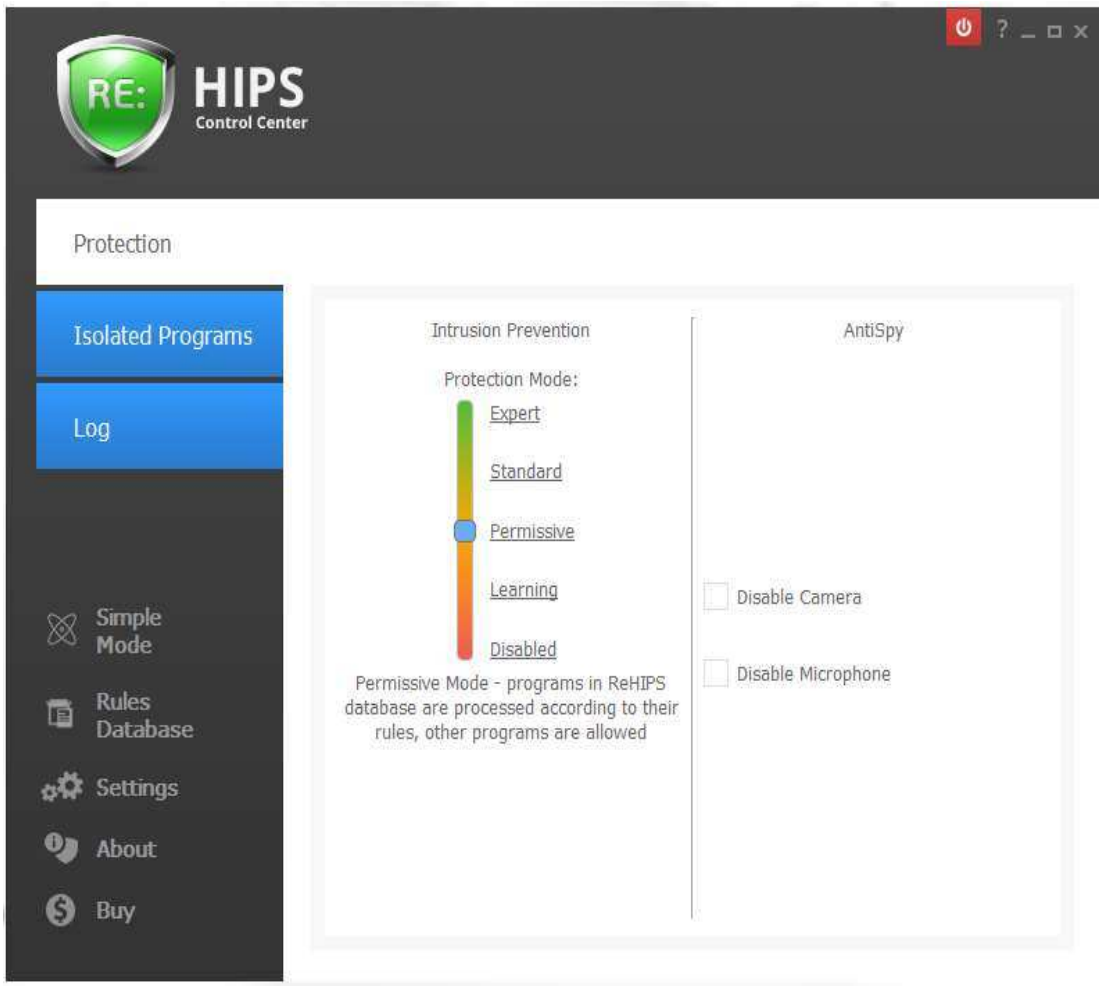
V rámci provedení výkonové a funkční komparativní analýzy byl jako testovací zařízení využit osobní počítač s aktuálním operačním systémem Windows 10 a s daným technickým vybavením:

- **Procesor:** Intel Core 2 Duo E4600 2,4 GHz
- **RAM:** 2 GB DDR2
- **HDD:** Seagate ST500NM0011 7200 RPM
- **Grafická karta:** NVIDIA GeForce GT 610 1GB DDR3 SDRAM
- **Síťová karta:** Qualcomm/Atheros L1 Gigabit Ethernet 10/100/1000Base-T Adapter
- **Router:** NETGEAR Nighthawk AC1900 Smart R700
- **Operační systém:** Windows 10 Pro 64 bit
- **Antivirový program:** ESET Internet Security 11.2.49.0

10.3 Vybrané řešení ReHIPS

Jedním z vybraných řešení HIPS pro analýzu byl vybrán program ReHIPS od firmy ReCryptCompany v demo verzi 2.4.0. Jedná se o inovativní řešení. Agenty není potřeba nijak speciálně nasazovat jako u jiných řešení, jsou už totiž registrovány hned po dokončení instalace. Uživatelské prostředí je zcela jednoduché a intuitivní. Vzhledem k situaci, že pro tuto bakalářskou práci byla použita pouze demo verze, je možné v jednom čase nasadit maximálně 10 izolovaných procesů. ReHIPS zajišťuje systémovou integritu a stabilitu.

Obrázek č. 7 znázorňuje uživatelské prostředí pro ReHIPS, kde v rámci ochrany AntiSpy lze vypnout funkci pro kameru či mikrofon. Prevence průniku obsahuje 5 režimů, mezi které patří Expert režim, Standard režim, Permissive režim, Learning režim a vypnutý režim. V rozšířeném nastavení lze zobrazit výpis logu.



Obrázek 7 - Uživatelské prostředí ReHIPS

Expertní režim (Expert) nabízí maximální ochranu, jakou je schopen zvládnout. Na Trusted Vendor list v tomhle režimu není brán zřetel. Disponuje zobrazováním velkého množství notifikací. [28]

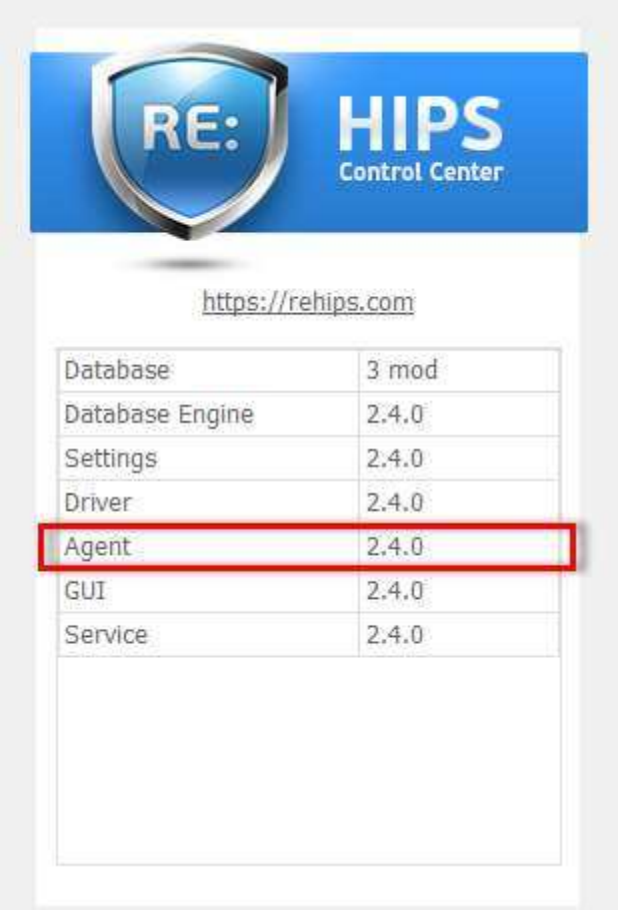
Standardní režim (Standard) je podobný expertnímu režimu, liší se ale v tom, že zobrazuje méně notifikací. Disponuje tím, že některé jeho aplikace jsou povoleny na základě heuristiky. [28]

Permissive režim umožňuje programům v databázi provedení na základě pravidel. [28]

Režim učení (Learning) uzpůsobuje pravidla programům, které jsou v databázi. Programy, které nejsou v databázi, mohou být povoleny a přidány do dané databáze. [28]

Vypnutý režim (Disabled) způsobí zastavení veškeré ochrany, kterou program nabízí.

Následující obrázek č. 8 zobrazuje zahrnutí agenta v daném programu.



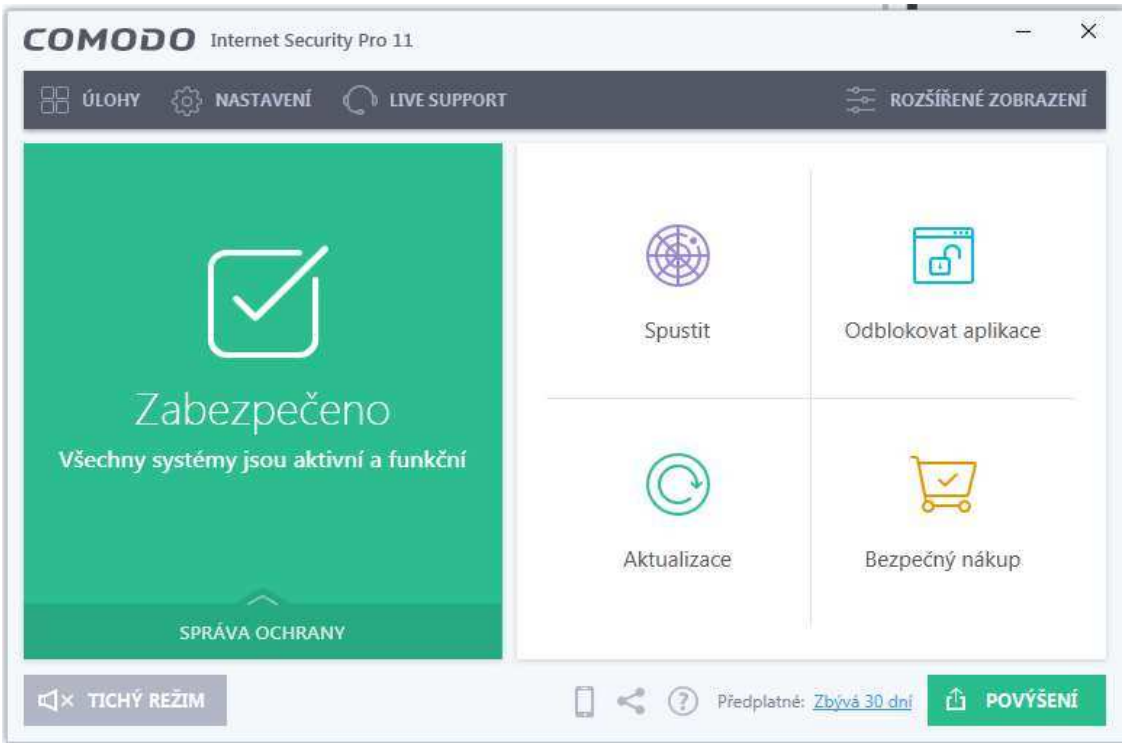
Obrázek 8 - agent obsažen v ReHIPS

10.4 Vybrané řešení Comodo Internet Security

Dalším z vybraných řešení HIPS pro analýzu byl vybrán Comodo Internet Security Pro od firmy Comodo. Jelikož se jedná o Pro edici, byla použita pro tuto bakalářskou práci pouze trial verze po dobu 30 dnů.

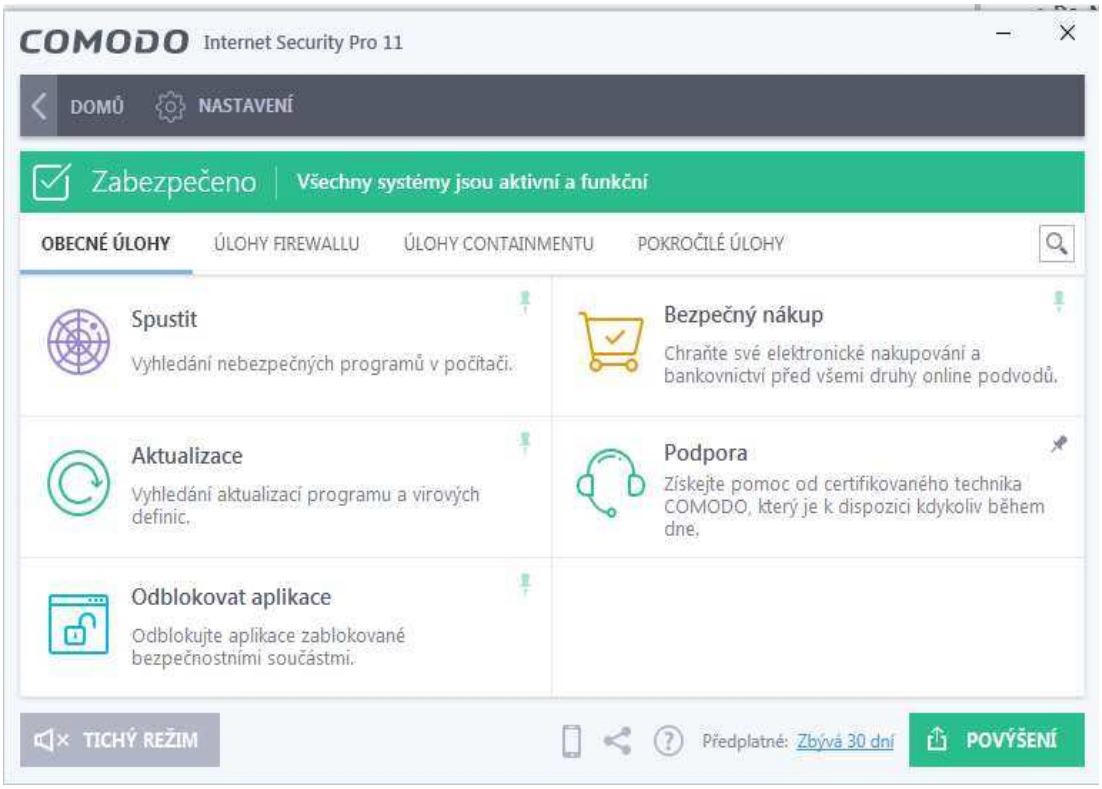
Comodo Internet Security je programem určeným ke zvýšené bezpečnosti sítě, který má HIPS technologií přímo obsaženou, tudíž není potřeba speciálním způsobem implementovat agenty, jako u jiných řešení.

Následující obrázek č. 9 zobrazuje úvodní prostředí pro Comodo Internet Security.



Obrázek 9 - Uživatelské prostředí COMODO Internet Security Pro

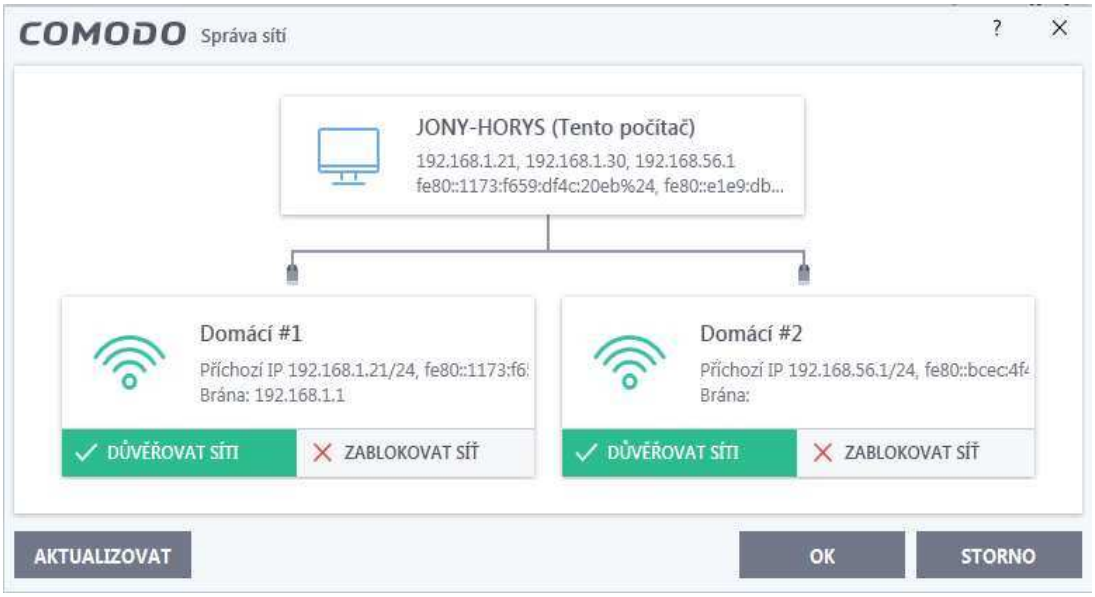
V levém horním rohu vidíme kartu úlohy, po jejím kliknutí vidíme další 4 bloky, které člení úlohy dle jejich činnosti, jak znázorňuje obrázek č. 10.



Obrázek 10 - karta úlohy

Úlohy jsou členěné na obecné úlohy, úlohy firewallu, úlohy containmentu a na pokročilé úlohy. Mezi obecnými úlohami jsou zařazené základní úlohy, které jsou zobrazeny i na úvodním prostředí. Konkrétně se tam nachází úloha pro spuštění kontroly, vyhledání aktualizací pro daný program, ochrana při online obchodování, odblokování aplikací, které byly zablokovány v rámci bezpečnostních akcí a speciální online podpora od odborných osob v rámci firmy COMODO.

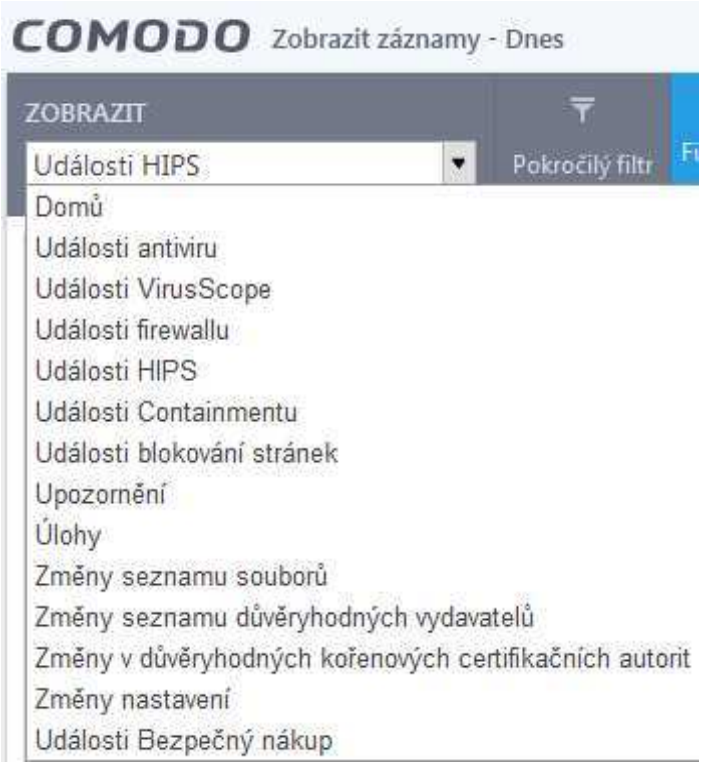
Mezi úlohami pro firewall najdeme úlohu pro povolení konkrétní aplikace k síťovému připojení a zároveň také zablokování konkrétní aplikace k síťovému připojení. Dále se zde nachází úloha pro zamaskování portu, čímž lze konkrétní zařízení učinit neviditelné pro ostatní elektronická zařízení, všechna příchozí spojení budou tedy blokována. V úlohách firewallu lze také zablokovat veškerou síťovou aktivitu či ji zpětně odblokovat dle potřeby. Následně je zde zařazena úloha pro zobrazení seznamu aplikací, které jsou v daném momentě připojeny k veřejné síti. A na závěr poslední úlohou firewallu je úloha pro správu sítí, kde lze povolit či zakázat spojení pro dostupnou počítačovou síť, jak znázorňuje obrázek č. 11.



Obrázek 11 - Správa sítí úloha

Následně se v kartě úlohy nachází úlohy pro containment, ve kterých lze spustit úlohu pro zabezpečenou virtuální plochu. Dále lze zobrazit podrobné informace o aktivních procesech, které jsou v daném momentě spuštěné na konkrétním elektronickém zařízení. Mezi dalšími úlohami pro containment jsou zařazeny úlohy pro otevření sdíleného prostoru mezi klasickými aplikacemi a mezi aplikacemi virtualizovanými, dále je zde možné spustit aplikaci virtualizovanou metodou v sandboxu a zabránit tak provádět trvalé změny v systému. Od této úlohy se odvíjí další úloha, která umožňuje sandbox obnovit, čímž vymaže všechen obsah kontejneru. Poslední úlohou pro containment je úloha pro sledování aktivity systému pro jednotlivý proces, toho lze učinit pouze za pomocí programového doplňku COMODO KillSwitch.

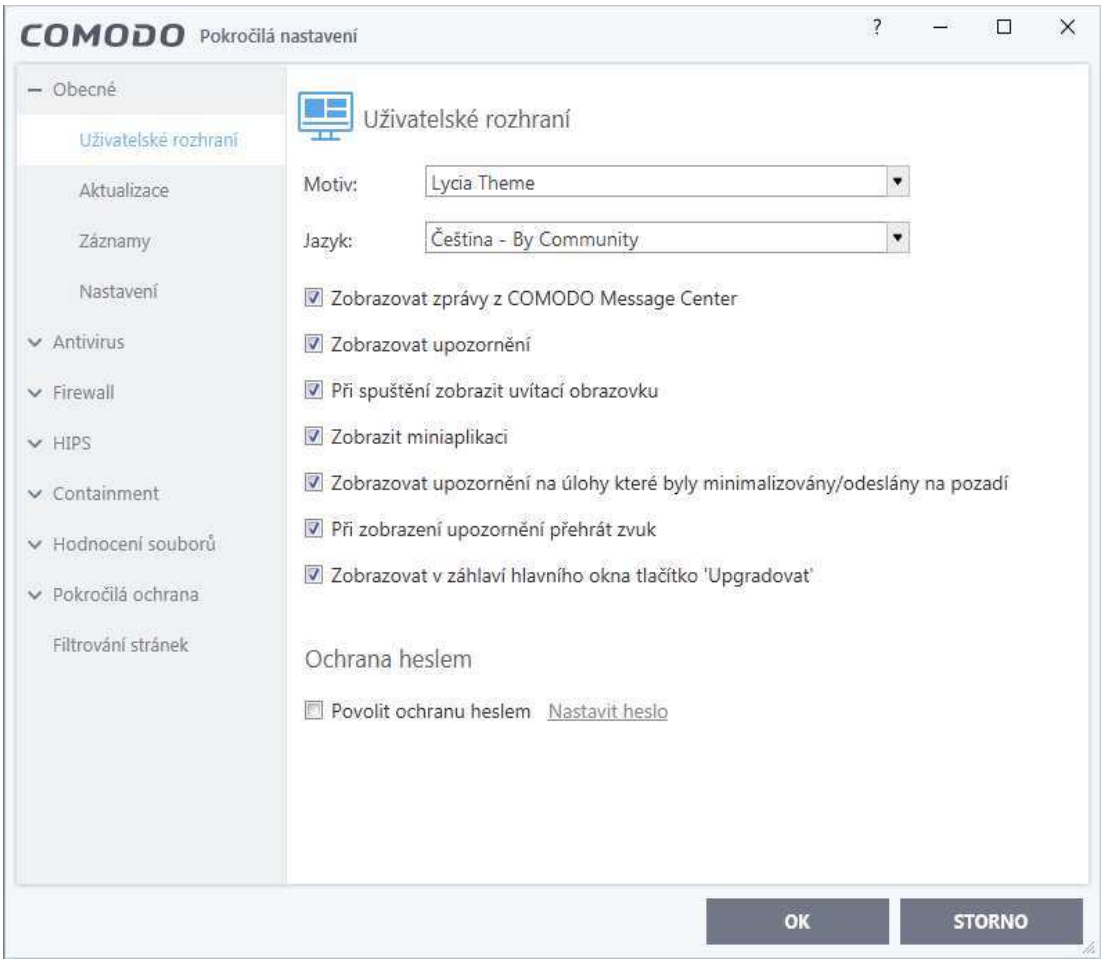
Posledním oddílem pro kartu úloh jsou pokročilé úlohy, mezi ně patří vytvoření záchranného disku, zobrazení záznamů, vyčištění koncových bodů, karanténa, zaslání souborů a klasický správce úloh, který sleduje a umožňuje správu konkrétních právě spuštěných úloh. Úloha pro zaslání souborů uzpůsobuje k provedení analýzy odeslání libovolného počtu dostupných souborů. Tato úloha také nabízí možnost k označení falešného poplachu pro konkrétní soubor. Úloha karanténa funguje jako prostředí určené pro prohlížení a správu určitých položek, které do ní byly umístěny. Úloha pro vyčištění koncových bodů je určena k vyčištění pro těžko odstranitelné infekce, čehož lze docílit pouze za pomocí programového doplňku COMODO Cleaning Essentials. Úloha pro vytvoření záchranného disku slouží k vytvoření spustitelného kompaktního disku (CD) či k USB flash disku, pro případné vyčištění nakaženého elektronického zařízení. Úloha pro zobrazení záznamů poskytuje prohlížení událostí, akcí a upozornění, které byly v minulosti zaznamenány. Záznamy je možné různě filtrovat a také exportovat do HTML souborů. Záznamy mají své členění dle konkrétního typu, jak znázorňuje obrázek č. 12. Uskupení obsahuje například události antiviru, událost firewallu, události containmentu nebo právě události HIPS, které jsou důležité pro tuto bakalářskou práci.



Obrázek 12 - Členění záznamů

Vedle karty úlohy v úvodním prostředí se nachází karta nastavení, která je znázorněná na následujícím obrázku č. 13.

Při otevření se zobrazí nejprve obecné nastavení, které se týká uživatelského rozhraní, aktualizací, záznamů a nastavení importu, exportu s přepínáním mezi profily nastavení.



Obrázek 13 - Pokročilé nastavení COMODO Internet Security Pro

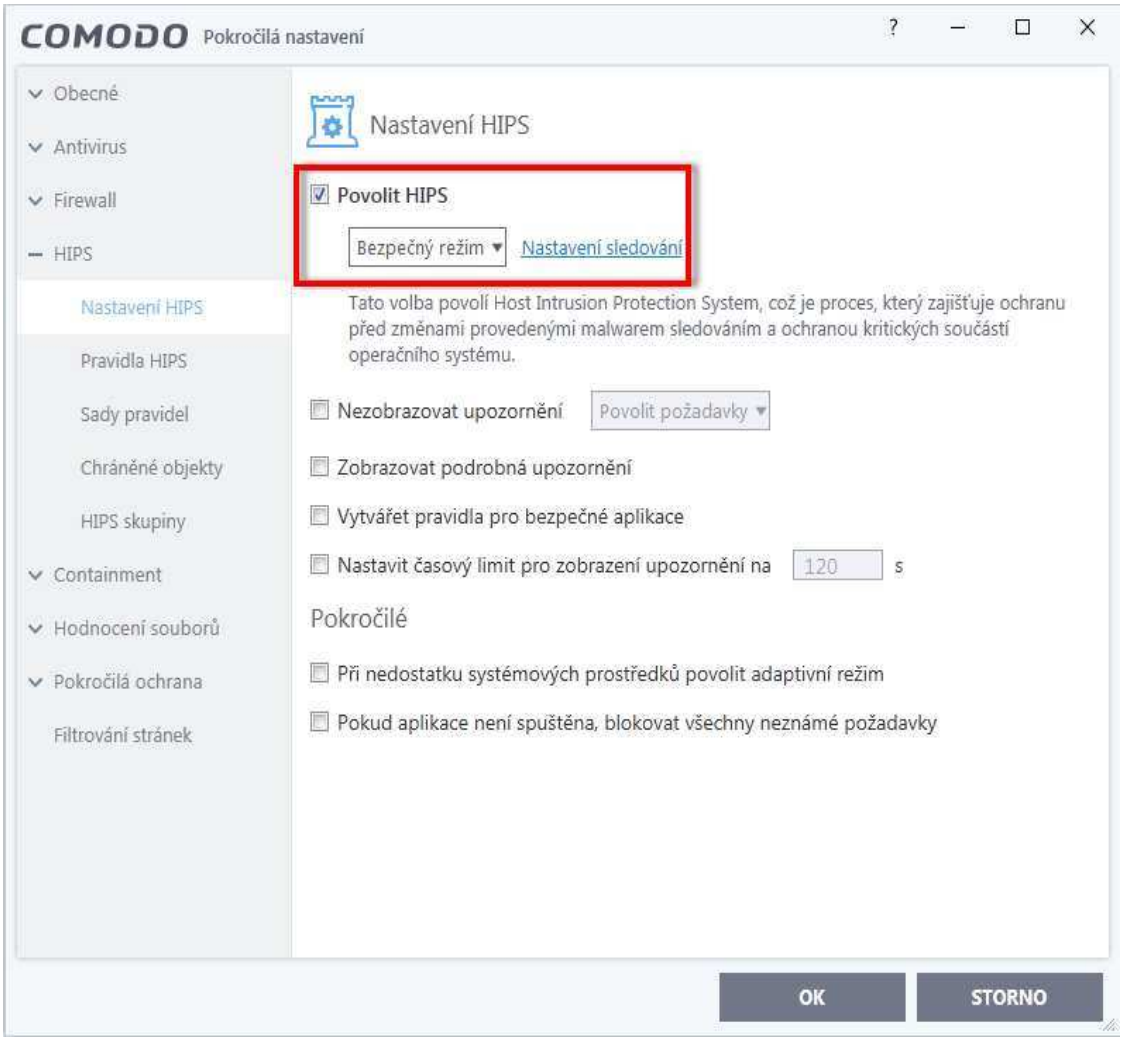
U antivirusu je umožněno nastavení pro rychlou kontrolu, úplnou kontrolu, ruční skenování a také nastavení rezidentní kontroly.

V rámci firewallu lze v nastavení povolit filtrování komunikace, nastavení upozornění, umožňuje také filtrování IPv6, filtrování loopback přenosů, blokování fragmentovaných IP přenosů, analýzu protokolů a ochranu vůči ARP spoofingu. Firewall má zde aplikační a globální pravidla, která lze upravovat. Disponuje zde sadou portů, které jsou definované pro konkrétní zařízení a těmi jsou HTTP port, POP3 porty, SMTP porty a privilegované porty.

Dále se zde nachází pokročilé nastavení containmentu, hodnocení souborů, filtrování stránek, pokročilá ochrana, ve které je možnost povolení VirusScope a hlavně pokročilé nastavení pro HIPS, které je pro tuto bakalářskou práci důležité.

Obrázek č. 14 zobrazuje okno pro pokročilé nastavení HIPS technologie.

Pro realizaci tohoto řešení je potřeba odfajfkovat zaškrtávací pole pro „Povolit HIPS“, jako tomu je na obrázku č. 14.



Obrázek 14 - nastavení HIPS pro Comodo Internet Security Pro

V nastavení HIPS technologie je možné vypnout upozornění nebo naopak zobrazit podrobné upozornění, můžeme také nastavovat časový limit, v případě možnosti zobrazení poskytnutého upozornění. Dále lze vytvářet pravidla pro bezpečné aplikace.

Pod zaškrtávacím polem pro povolení HIPS technologie se nachází výběr tří režimů. Mezi dostupnými třemi režimy se vyskytuje bezpečný režim, paranoidní režim a režim učení.

Paranoidní režim je nejvyšší úroveň zabezpečení. V tomto režimu HIPS sleduje a má kontrolu nad všemi spustitelnými soubory, výjimkou jsou pouze soubory, které jsou chápány jako dostatečně bezpečné. Jedná se o režim, který vytváří nejvíce upozornění.

Nevytváří samovolně možnosti povolení jednotlivých pravidel, ale i přesto poskytuje možnosti úprav dle uživatele. [33]

Režim učení je založen na sledování a učení se aktivity všech možných spustitelných souborů, kterým vytváří samovolně možnosti povolení. Tímto způsobem se zásadně liší od paranoidního režimu. Dále se od něj liší tím způsobem, že od HIPS technologie nevytváří žádná upozornění. V tomto režimu je zapotřebí mít vědomí o dostatečné bezpečnosti všech spustitelných souborů a aplikací. [33]

Bezpečnostní režim se v průběhu sledování kritických činností konkrétního systému automaticky učí aktivitu všech možných spustitelných souborů či aplikací, stejně jako tomu je u režimu učení. Zde u tohoto režimu jsou však dané spustitelné soubory či aplikace označeny od firmy Comodo za dostatečně bezpečné. V opačném případě, kdy některé spustitelné soubory či aplikace nejsou označené za dostatečně bezpečné, systém dostane upozornění, pokud by mělo dojít k jejich spuštění. Možnost povolení vytváří pouze v případě, pokud je označeno zaškrtávací pole pro vytvoření pravidel pro bezpečné aplikace.

Vedle výběru jednoho ze tří režimů je odkaz na nastavení sledování, jehož okno znázorňuje obrázek č. 15.

Mezi sledovanými aktivitami se nachází meziprocesní přístup k paměti, okenní zprávy, spouštění procesů, ukončení procesů, instalace ovladačů zařízení, Windows/WinEvent háčky a služba pro klienta DNS/RPC.

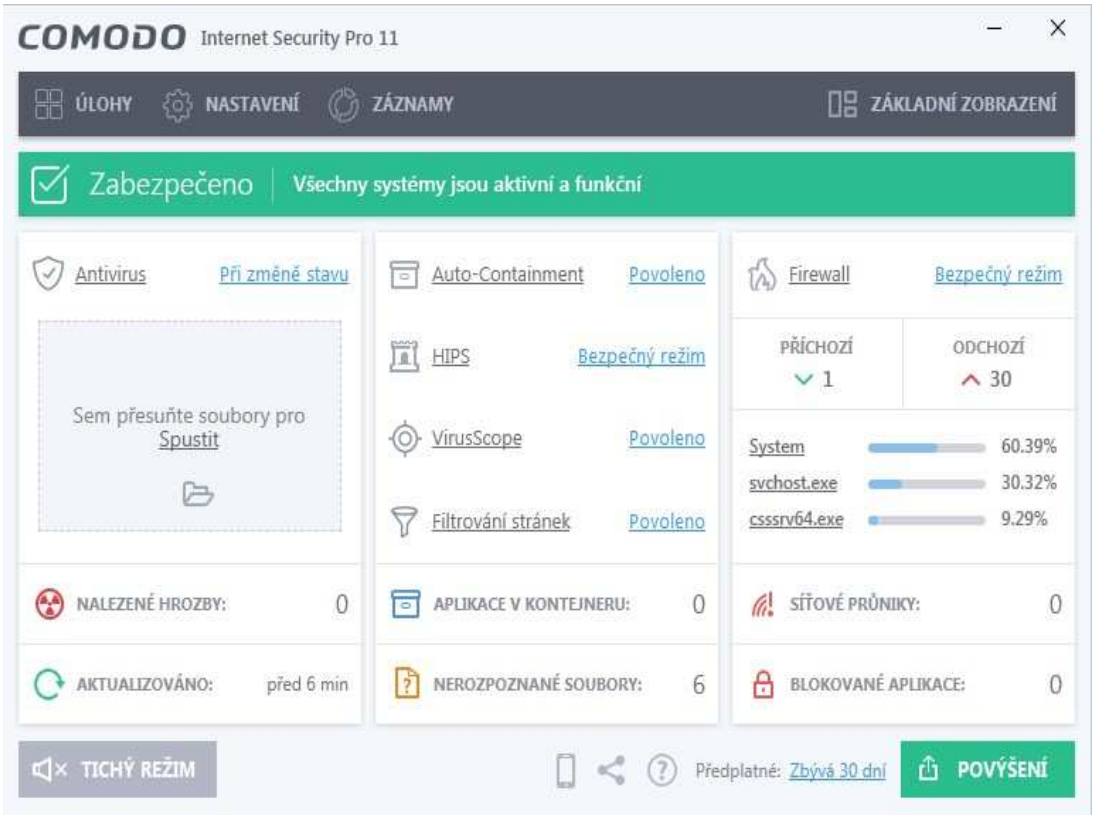
Proti přímému přístupu jsou chráněné disky, fyzické paměti, monitory, klávesnice, a proti úpravám jsou chráněné klíče registrů, soubory a COM rozhraní.

Obrázek 15 - Nastavení sledování pro Comodo Internet Security Pro

Na úvodním okně pro uživatelské prostředí v pravém horním rohu je možnost rozšířeného zobrazení, jehož náhled znázorňuje obrázek č. 16.

Vidíme zde, že je povoleno HIPS řešení a to v bezpečném režimu, což je pro tuto bakalářskou práci nezbytně důležité.

Je zde také vidět i nastavení bezpečného režimu pro firewall, zároveň je povoleno filtrování stránek, technologie VirusScope a Auto-Containment.



Obrázek 16 - rozšířené zobrazení COMODO Internet Security Pro

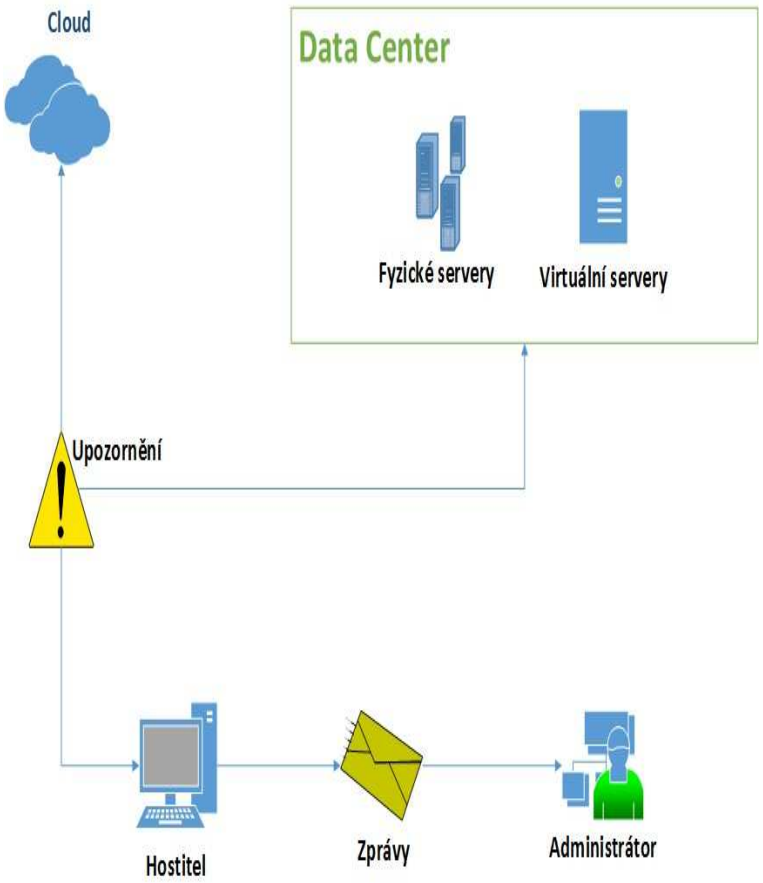
10.5 Vybrané řešení DeepSecurity

Další vybraným řešením HIPS pro analýzu bylo vybráno DeepSecurity ve verzi 9.6. Jedná se o multiplatformní řešení, od firmy Trend Micro. K provedení analýzy byla realizována pouze trial verze, která byla pro tuto bakalářskou práci zcela dostačující. Během instalace bylo k dokončení testu nutné vybrat, jaký typ databáze se využije. Na výběr byl Microsoft SQL, Oracle, PostgreSQL a vestavěná databáze Apache. Pro tuto práci byla vybrána vestavěná databáze Apache. DeepSecurity, prostředí je také vybaveno management serverem, který funguje s webovým rozhraním.

Klíčovými přednostmi DeepSecurity pro business sféru jsou zabezpečení virtuálních desktopů, zabezpečení cloudového prostředí a hlavně zabezpečení serverů, ať už se jedná o fyzické, virtuální či cloudové. [24]

DeepSecurity je optimalizovaný pro prostředí VMware, Amazon Web Services a Microsoft Azure.[23]

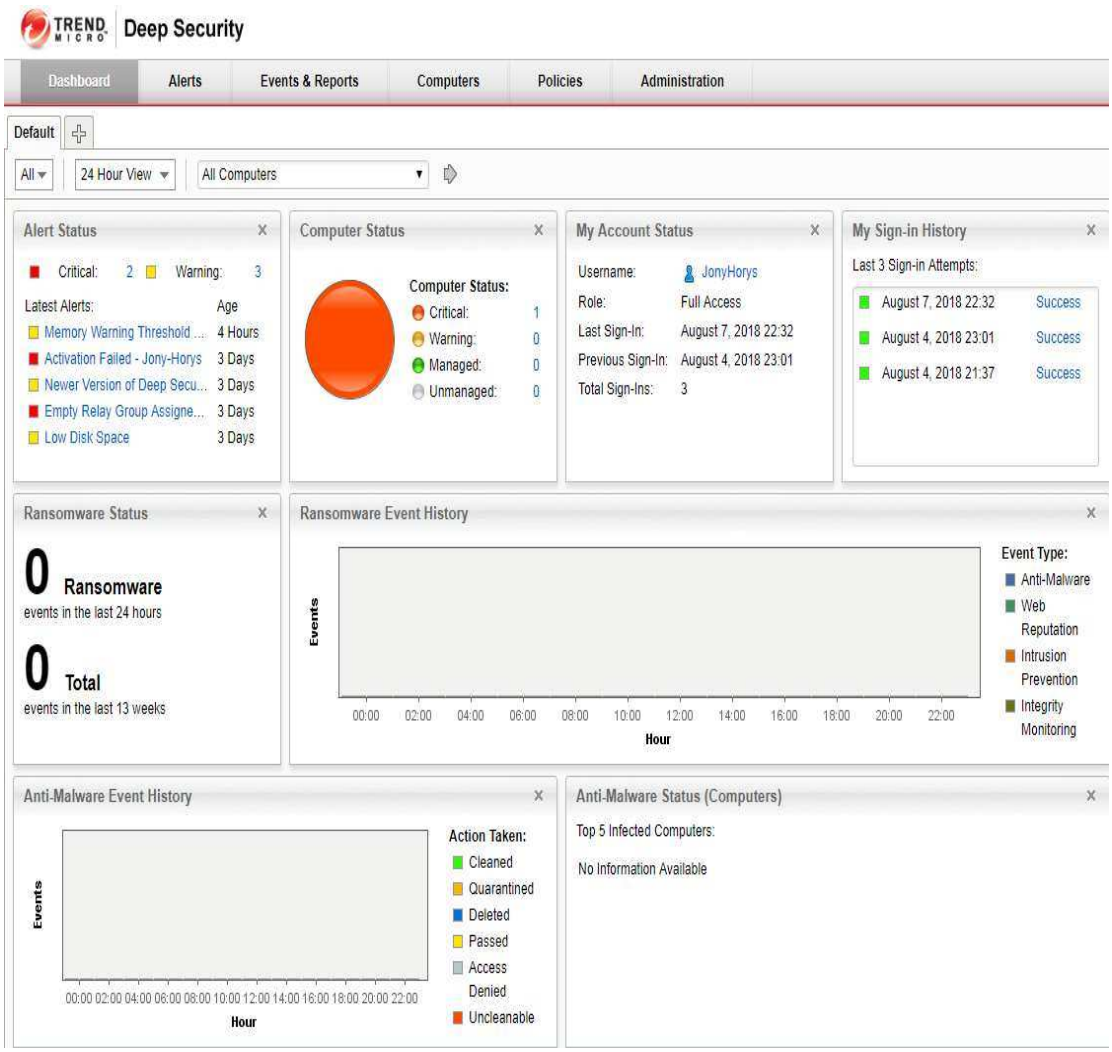
Kromě činností prevence průniku, které souvisí s touto bakalářskou prací, DeepSecurity je také schopen fungovat jako Anti-Malware, Firewall, kontrolor logů a kontrolor integrity souborů.



Obrázek 17 - Fungování DeepSecurity v praxi

Přepracováno od Zdroje: Trend Micro DeepSecurity Data Center

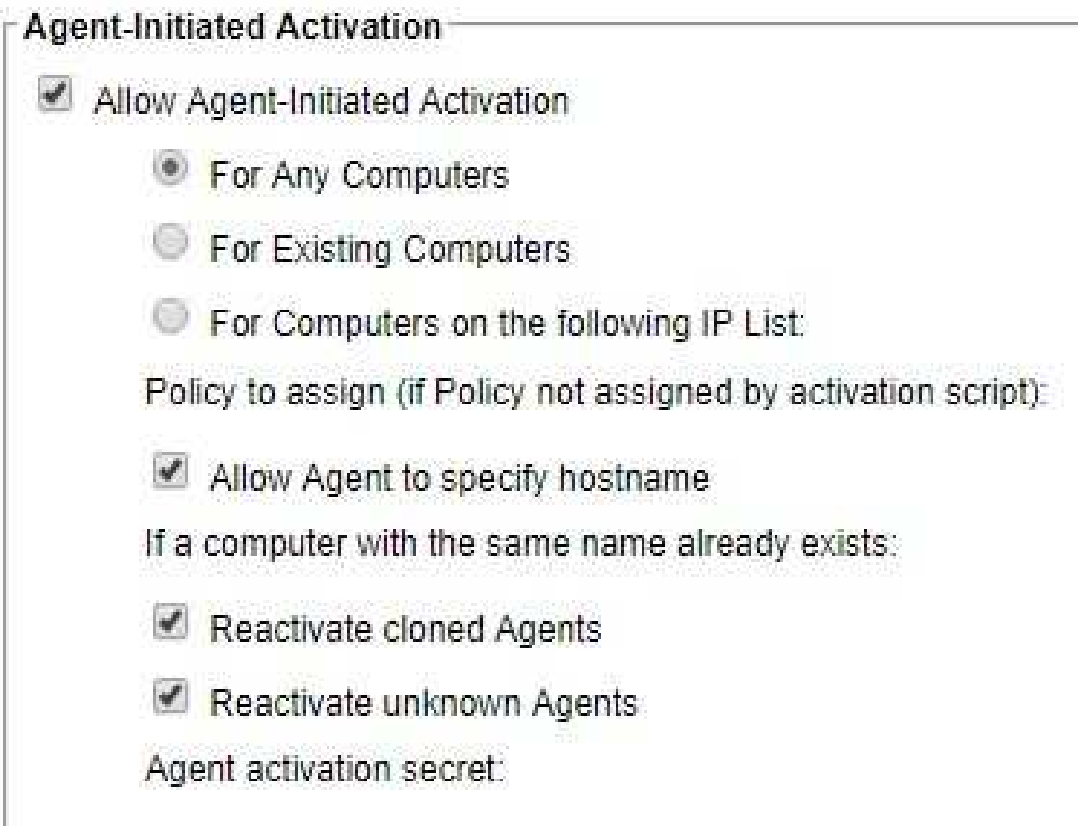
Následující obrázek č. 18 znázorňuje úvodní stránku, neboli dashboard DeepSecurity management serveru, který je pro uživatele dostupný přes webové rozhraní. Na dané úvodní stránce vidíme stav upozornění, kde se například zobrazují kritické či výstražné zprávy ohledně aktivit. Vedle také vidíme stav počítače či elektronického zařízení znázorněný v kruhovém, neboli koláčovém grafu. Následně tu vidíme stav uživatelského účtu a historii přihlášení do tohoto prostředí. Dole máme zobrazené jednotlivé historie konkrétních událostí, jimiž je například na obrázku zachycená událost ohledně anti-malware činnosti, dále tam vidíme historii událostí ohledně činností firewallu, systému prevence průniku, webové reputace, kontrola logů a kontrola integrity souborů.



Obrázek 18 - webové uživatelské prostředí Deep Security

Na konkrétní testovací zařízení byli implementováni agenti.

Agenti byli aktivováni v systémovém nastavení management serveru, jak znázorňuje obrázek č. 19., pro agenty byly nastaveny patřičné politiky.



Obrázek 19 - aktivace agenta v DeepSecurity

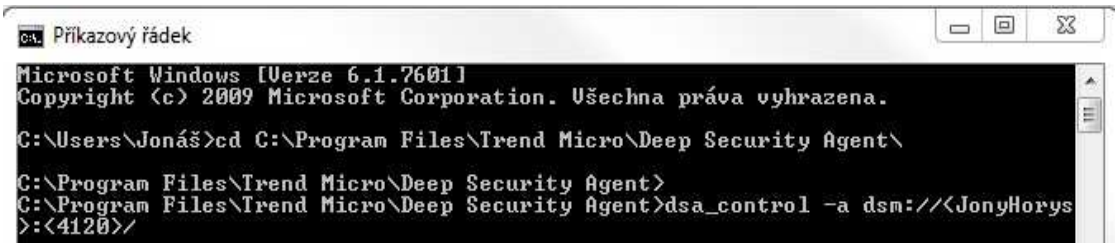
Agenty lze aktivovat také prostřednictvím příkazového řádku a to následujícími příkazy.

cd C:\Program Files\Trend Micro\DeepSecurity Agent\

dsa_control -a dsm://<host>:<port>/

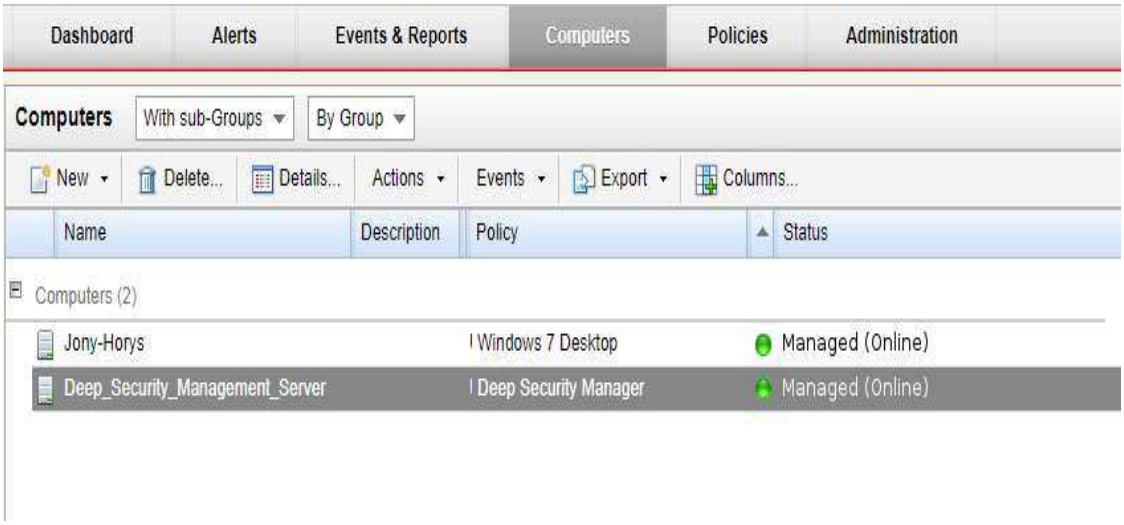
První řádek příkazu udává vstup do adresáře na daném testovacím zařízení pro agenta DeepSecurity.

Druhý řádek příkazu udává potřebnou aktivaci agenta. Část příkazu „dsa_control“ je určena ke konfiguraci agenta. Znak „-a“ je určen k aktivaci daného agenta. Do části „<host>“ se uvádí buď doménové jméno Managera, nebo IP adresa. A do poslední části „<port>“ se uvádí číslo síťového portu, kterým v tomhle případě bývá většinou číslo 4120.



Obrázek 20 - ukázka aktivace agenta v rámci CLI

Následující obrázek č. 21 zobrazuje implementované agenty v management serveru a na testovacím zařízení pro operační systém Windows. V této části prostředí je možné nejenom aktivovat jednotlivá zařízení, je zde také umožněno členění do skupin, skenování portů, zobrazení stavu, přiřazení politik, vymazání historie upozornění či chyb, přiřazení hodnot a přiřazení do Relay skupiny. Přiřazení do Relay skupiny umožňuje defaultně stahovat aktualizace potřebných modulů konkrétnímu zařízení. Lze také zobrazit informace ohledně událostí na vybraném zařízení, činností Anti-malwaru, prevence průniku, firewallu, webové reputace, kontroly logů, kontroly integrity a také systémové události.



Obrázek 21 - nasazení agenta na testovací zařízení

11 Komparativní analýza vybraných řešení HIPS

Na základě provedení komparativní analýzy pro tři vybraná řešení HIPS, kterými jsou Comodo Internet Security Pro, ReHIPS a DeepSecurity, byla zohledněna jednoduchost prostředí, konfigurace, účinek při prevenci průniku, realizace v prostředí podniku, možnosti či specifické určení.

Prvním vybraným řešením byl Comodo Internet Security Pro, který měl vcelku intuitivní úvodní prostředí s bohatými možnostmi nastavení pro zabezpečení. Je jediným řešením, které mělo k dispozici českou lokalizaci. S množství funkcí a možností rozhodně převyšoval druhé řešení ReHIPS. Dané řešení je vhodné pro domácnost s větším počtem zařízení či malý podnik. Pro větší podniky je rozhodně nejvíce aplikovatelné řešení DeepSecurity.

Druhým vybraným řešením byl ReHIPS, který měl v porovnání s ostatními řešeními s jistotou nejjednodušší konfiguraci a ze všech řešení nejvíce jednoduché prostředí. Naproti tomu je vybaven malým obsahem možností a funkcí, kde ho další dvě řešení ve srovnání nadměrně převyšují. Toto řešení je vhodné spíše pro jednotlivce, pro osobní použití, než pro implementaci v prostředí podniku. Jedná se také o cenově nenáročné řešení.

Poslední vybrané řešení bylo DeepSecurity od firmy Trend Micro, které mělo rozhodně v porovnání s předchozími řešeními nejsložitější konfiguraci. Agenti se museli zvlášť implementovat, zatímco předchozí řešení měla agenty už implicitně obsažené. Ovšem pro implementaci do prostředí podniku se vzhledem k možnostem a funkcím z těchto tří vybraných řešení hodí nejvíce. Od toho se také odráží zjištění, že se při plné licenci na delší dobu jedná o cenově nejnáročnější řešení. Z vybraných tří produktů se jedná o nejúčinnější řešení při prevenci průniku.

12 Výkonová analýza dostupných řešení HIPS

Mimo komparativní analýzy byla provedena následně výkonová analýza. Výkonová analýza se odvíjela od toho, jak moc bylo testovací zařízení průměrně vytížené v rámci procesoru (CPU), operační paměti (RAM), swapovacího oddílu (SWP), kolik kapacity zabíral instalační balík a jaká kapacita produktu byla po instalaci. Všechna řešení byla aplikovaná pod jedním desktopovým operačním systémem a tím byl 64 bitový Windows 10 v edici Pro.

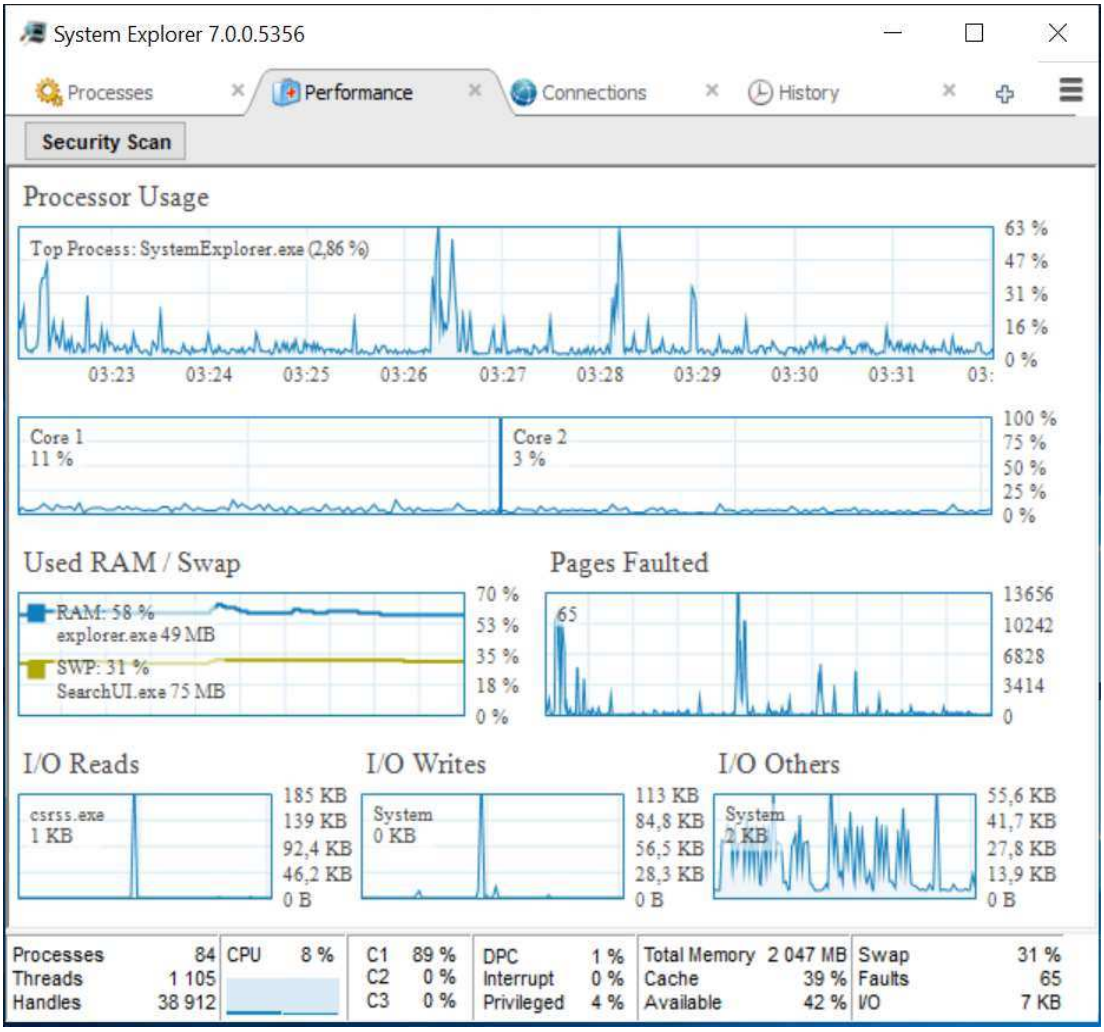
Jako nástroj pro měření výkonu testovaného zařízení při běhu vybraných HIPS řešení byl použit volně dostupný program nazývající se System Explorer. Nástroj Systém Expoler nám zobrazuje přehledné informace o procesech, službách, úkolech, probíhajících aplikacích a hlavně poskytuje podrobné sledování výkonu ohledně procesoru (CPU), operační paměti (RAM) a swapovacího oddílu (SWP). Což je pro tuto bakalářskou práci důležité.

Před aplikováním měření výkonu testovacího zařízení při běhu jednotlivých HIPS řešení se nejdříve sledoval výkon daného zařízení v počátečním stavu. To znamená, že při běhu operačního systému Windows byly spuštěny pouze nezbytné prvky pro fungování operačního systému, antivirový program ESET Smart Security a samozřejmě utilita System Explorer.

12.1 Sledování výkonu v počátečním stavu

Následující obrázek č. 22 znázorňuje průměrné vytížení testovacího zařízení v době přibližně deseti minut při počátečním stavu. Testování výkonu počátečního stavu probíhalo od 3:22 do 3:32.

Průměrné vytížení procesoru (CPU) se pohybovalo během přibližných deseti minut okolo hodnoty 10%.
Průměrné vytížení operační paměti (RAM) se pohybovalo během přibližných deseti minut okolo hodnoty 58%. Průměrné vytížení swapovacího oddílu (SWP) se pohybovalo na hodnotách okolo 31%.



Obrázek 22 - Sledování výkonu v počátečním stavu

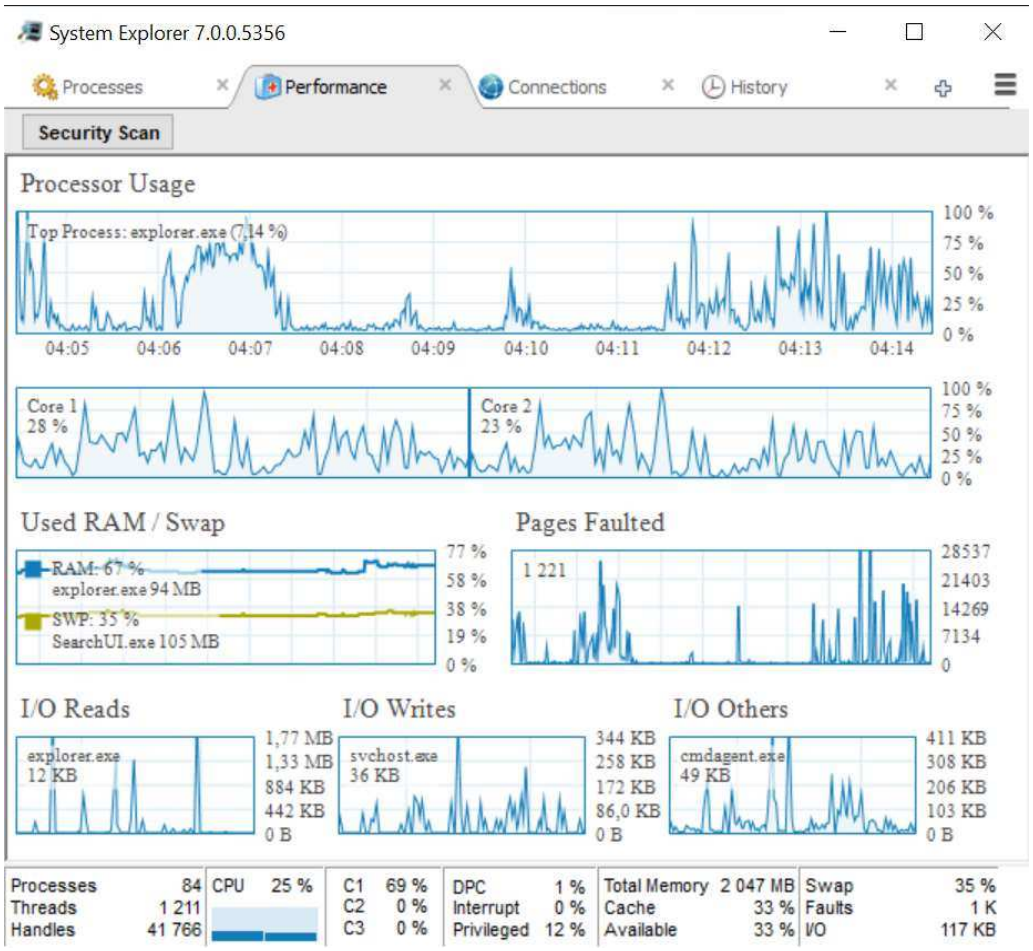
12.2 Sledování výkonu pro řešení Comodo Internet Security Pro

Následující obrázek č. 23 znázorňuje průměrné vytížení testovacího zařízení v době přibližně deseti minut při běhu řešení Comodo Internet Security Pro. Testování výkonu při běhu Comodo Internet Security Pro probíhalo zhruba v čase od 4:05 do 4:15 hodin.

Průměrné vytížení procesoru (CPU) se pohybovalo během přibližných deseti minut okolo hodnoty 50%, což bylo nejspíše zapříčiněno i tím, že v průběhu sledování byla spuštěna rychlá kontrola.

Průměrné vytížení operační paměti (RAM) se pohybovalo během přibližných deseti minut okolo hodnoty 67%, což znamená, že se zvedlo zatížení na operační paměť (RAM) o 9%, oproti počátečnímu stavu. Průměrné vytížení swapovacího oddílu (SWP) se pohybovalo na hodnotách okolo 35%.

Kapacita instalačního balíku byla přibližně 5,5 MB, po instalaci dosahoval produkt kapacity přibližně 290 MB. Instalace na daném testovacím zařízení trvala přibližně 15 minut.



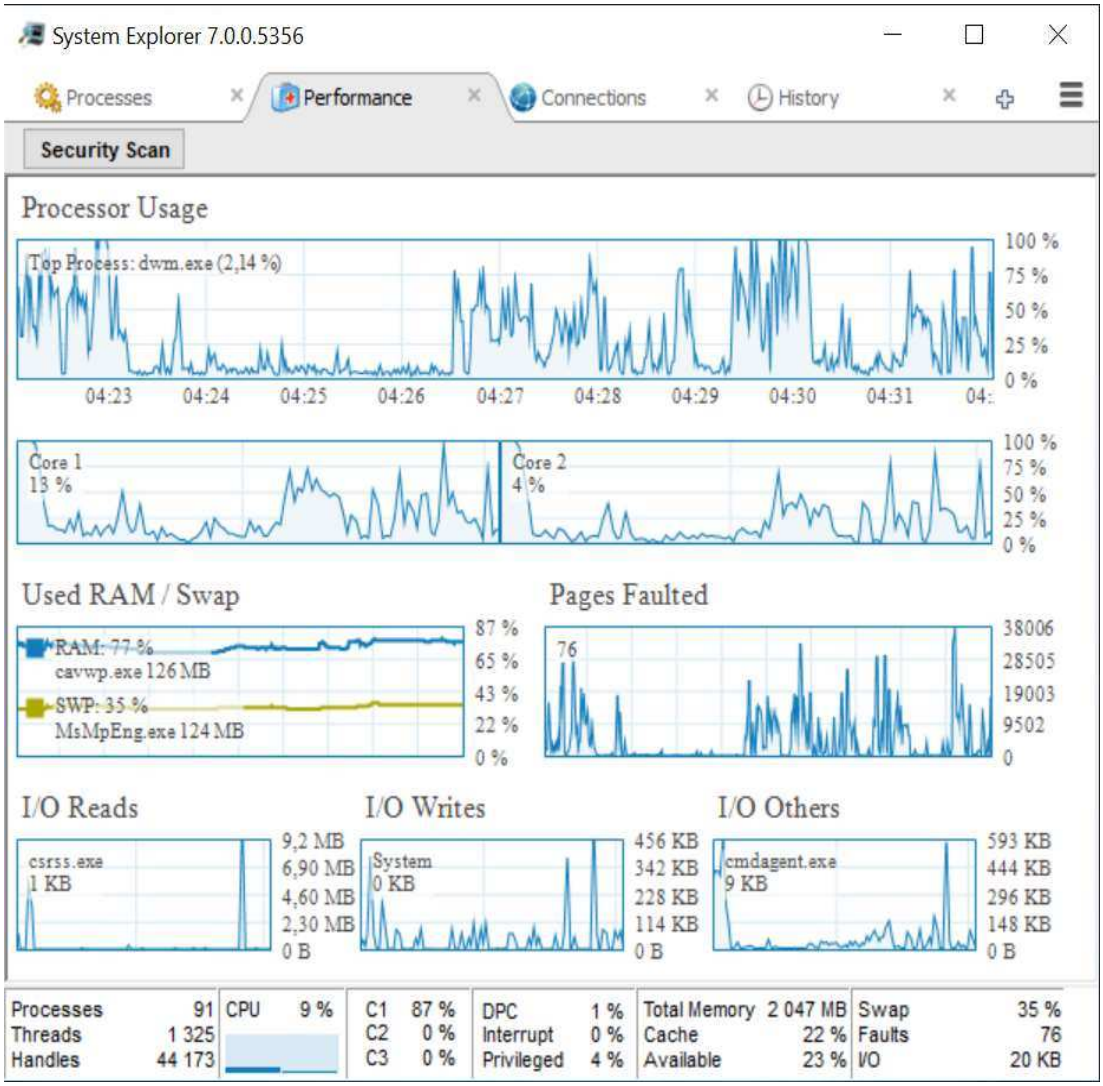
Obrázek 23 - sledování výkonu při běhu Comodo

12.3 Sledování výkonu pro řešení ReHIPS

Následující obrázek č. 24 znázorňuje průměrné vytížení testovacího zařízení v době přibližně deseti minut při běhu řešení ReHIPS. Testování výkonu při běhu ReHIPS probíhalo zhruba v čase od 4:22 do 4:32 hodin.

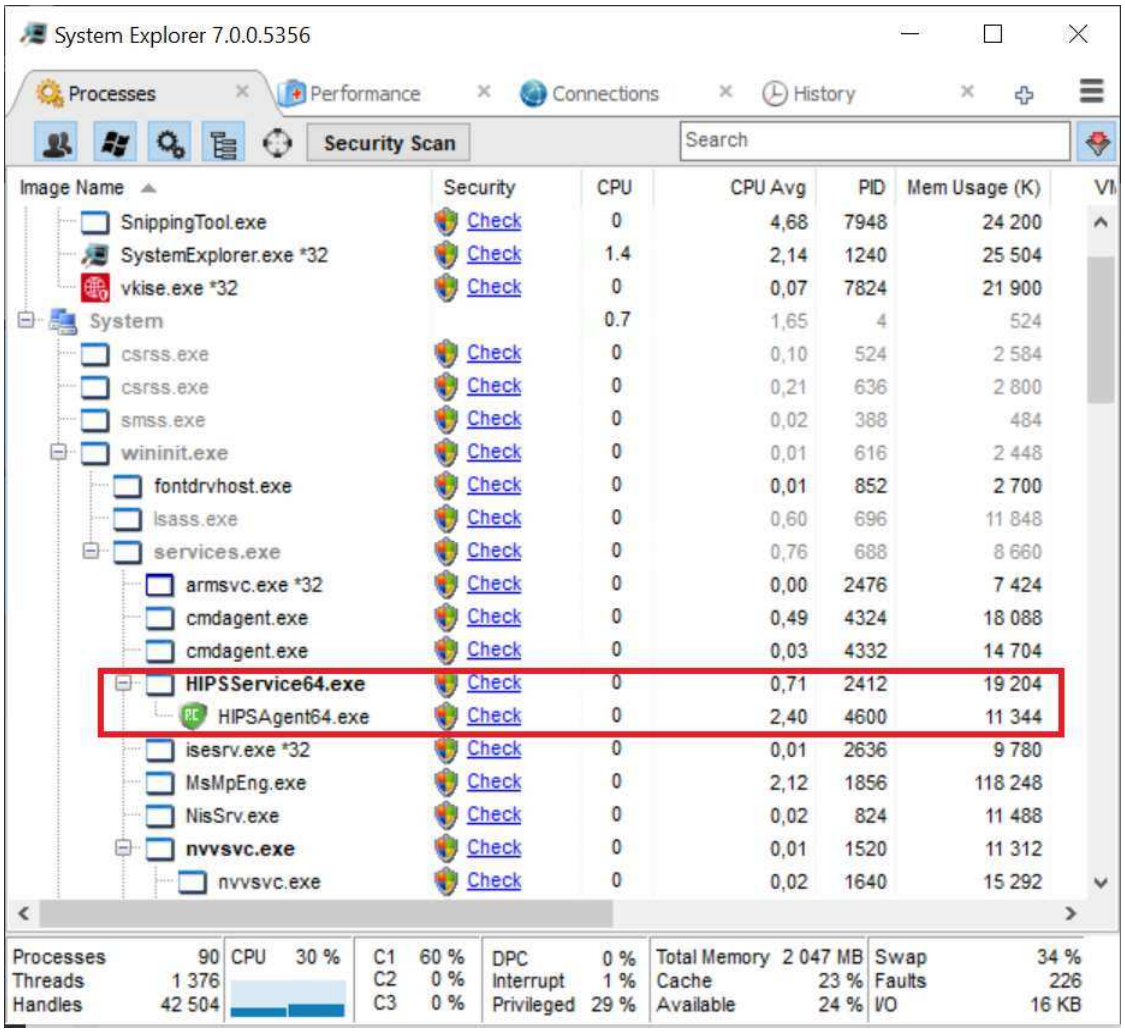
Průměrné vytížení procesoru (CPU) se pohybovalo v průběhu přibližných deseti minut okolo hodnoty 60%.
Průměrné vytížení operační paměti (RAM) se pohybovalo v průběhu přibližných deseti minut okolo hodnoty 72%, což znamená, že se zatížení operační paměti (RAM) zvedlo poměrně zanedbatelně, stejně jako tomu bylo u řešení pro Comodo Internet Security Pro.

Kapacita instalačního balíku byla přibližně 36 MB, po instalaci dosahoval produkt kapacity přibližně 74,1 MB. Instalace na daném testovacím zařízení trvala přibližně 14 minut.



Obrázek 24 - Sledování výkonu při běhu ReHIPS

Obrázek č. 25 znázorňuje, jakou hodnotu zabere aplikace a agent pro ReHIPS dle implicitního správce úloh ve Windows, což je přibližně 30,5 MB, takže není znepokojující, že dané řešení nemá na zatížení skoro žádný vliv.



Obrázek 25 - ReHIPS agent a aplikace zatížení ve správci úloh

12.4 Sledování výkonu pro řešení DeepSecurity

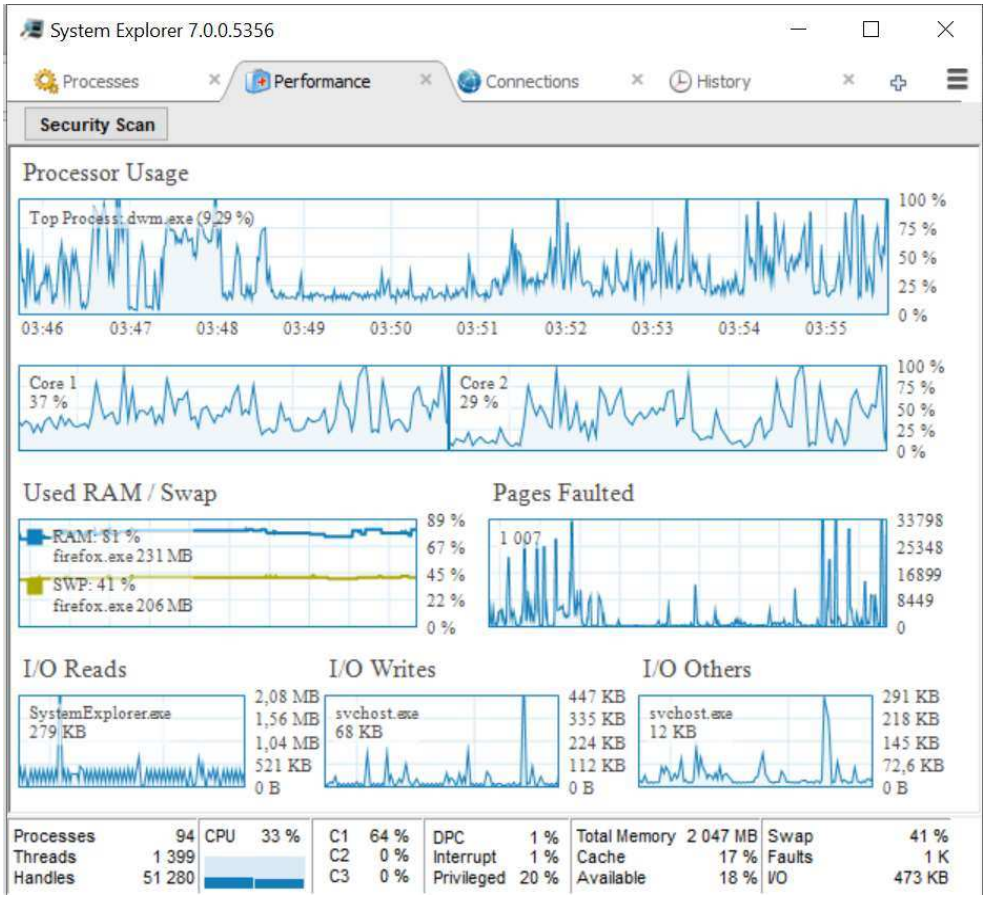
Následující obrázek č. 26 znázorňuje průměrné vytížení testovacího zařízení v době přibližně deseti minut při běhu řešení DeepSecurity. Testování výkonu při běhu DeepSecurity probíhalo zhruba v čase od 3:45 do 3:55 hodin.

Průměrné vytížení procesoru (CPU) se pohybovalo během přibližných deseti minut okolo hodnoty 75%, místy dosáhlo i na hranici 100%, zde byla poznat zásadní změna vůči počátečnímu stavu.

Průměrné vytížení operační paměti (RAM) se pohybovalo během přibližných deseti minut okolo hodnoty 81%, což znamená, že se zatížení operační paměti (RAM) zvedlo celkem výrazně, oproti předchozím řešením. Průměrné vytížení swapovacího oddílu (SWP) se pohybovalo na hodnotách okolo 44%.

Kapacita instalačního balíku byla přibližně 266,1 MB, po instalaci dosahoval produkt kapacity přibližně 1,18 GB. Instalace na daném testovacím zařízení trvala přibližně 31minut.

Z výsledků výkonové analýzy je zcela patrné, že největší zátěž na systémové prostředky nese řešení DeepSecurity. Vzhledem k tomu, že jeho uživatelské prostředí bylo spuštěno přes webový prohlížeč, bude to mít na zátěž rovněž dopad. Velký vliv na zatížení daného zařízení má předmětné řešení proto, že má oproti předešlým řešením rozsáhlé možnosti a správu programu.



Obrázek 26 - Sledování výkonu při běhu DeepSecurity

13 Vyhodnocení hypotézy

Na základě stanovení výchozích hypotéz bylo provedeno vyhodnocení testovaných řešení. Hypotéza se odvíjela od průměrného vytížení procesoru (CPU), průměrného vytížení operační paměti (RAM), průměrného vytížení swapovacího oddílu (SWP), kapacity instalačního balíku, velikosti kapacity po instalaci a od průměrné doby, jak dlouho trvala instalace na konkrétním testovacím elektronickém zařízení.

Sledování výkonu u každého řešení bylo opakováno třikrát a výsledky byly při každém pokusu podobné.

Tabulka č. 1 znázorňuje vyhodnocení pro každé z vybraných řešení při stanovených kritériích.

Tabulka 1 - Vyhodnocení hypotézy

	Comodo Internet Security Pro	ReHIPS	DeepSecurity
Průměrné vytížení CPU	50%	60%	75%
Průměrné vytížení RAM	67%	72%	81%
Průměrné vytížení swapovacího oddílu (SWP)	35%	35%	44%
Kapacita instalačního balíku	5,5 MB	36 MB	266,1 MB
Velikost kapacity po instalaci	290 MB	74,1 MB	1,18 GB
Doba trvání instalace	15 minut	14 minut	31 minut

Následující tabulka č. 2 znázorňuje komplexní porovnání všech tří řešení v rámci technického a subjektivního hodnocení zároveň. Číslo jedna značí nejlepší ohodnocení a číslo tři nejhorší ohodnocení. Hodnocení „1 (2)“ značí vyrovnané vyhodnocení. U hodnot zjištěných na základě sledování výkonu značí vyšší zjištěná hodnota horší hodnocení, protože se jedná o větší zátěž na konkrétní zařízení.

Tabulka 2 - Komplexní vyhodnocení

	Comodo Internet Security Pro	ReHIPS	DeepSecurity
Jednoduchost prostředí	2	1	3
Rozsah možností	2	3	1
Jednoduchost konfigurace	2	1	3
Realizace v prostředí podniku	2	3	1
Účinek při prevenci průniku	2	3	1
Cena / 1 rok	1	2	3
Cena / 2 roky	2	1	3
Průměrné vytížení CPU	1	2	3
Průměrné vytížení RAM	1	2	3
Průměrné vytížení swapovacího oddílu (SWP)	1 (2)	1 (2)	3
Kapacita instalačního balíku	1	2	3
Velikost kapacity po instalaci	2	1	3
Doba trvání instalace	2	1	3

V rámci vyhodnocení dle stanovených kritérií se stal produkt DeepSecurity od firmy Trend Micro ve všech ohledech tím nejnáročnějším produktem ze všech vybraných řešení. Je to způsobeno jeho rozsáhlostí oproti zbylým dvěma vybraným produktům. Jedná se o nejúčinnější produkt při prevenci průniku z těchto tří zvolených.

14 Licenční politika

Ekonomický dopad na implementaci a veškeré uzpůsobení určitého HIPS řešení je pro prostředí podniku nákladné nejen v pořízení daného softwaru. Náklady pro podnik zahrnují také cenu instalace a konfigurace od odborně způsobilé osoby, proškolení pracovníků, náklady na energii, náklady na údržbu a také na technické vybavení, aby se mohla implementace vůbec realizovat.

Co se týče ceny licencí jednotlivých řešení, tak u každého řešení je cena jinak uzpůsobena. Plnohodnotná licence pro ReHIPS stojí přibližně 1480 Kč a doba platnosti je neomezená.

Cena licence pro COMODO Internet Security Pro vychází přibližně na 910 Kč po dobu jednoho roku pro tři zařízení.

Poslední nejnáročnější řešení DeepSecurity má cenu licence rozdělenou podle rozsahu nasazení a technologií v daném podniku. U tohoto řešení jsou ceny udávané podle hodin využití, to se cenově člení na 0,01$, 0,03$ a 0,06$.

Tabulka 3 - Náklady na zisk dané licence po dobu 1 roku

	COMODO Internet Security Pro	ReHIPS	DeepSecurity
Licence	910 Kč	1480 Kč	1995 Kč (v případě nejlevnější varianty)

Cena pro DeepSecurity byla vypočtena tak, že se zvolil nejmenší rozsah, který vyšel na cenu 0,01$ za hodinu a vynásobil se číslem 24 (hod/den) a 365 (den/rok).

Tabulka 4 - Náklady na zisk dané licence po dobu 2 let

	COMODO Internet Security Pro	ReHIPS	DeepSecurity
Licence	1820 Kč	1480 Kč	3990 Kč (v případě nejlevnější varianty)

Tabulka č. 3 zobrazuje, že cena na pořízení licence na jeden rok se nijak značně neliší, když se vezme v úvahu, že v případě DeepSecurity byl zvolen ten nejlevnější způsob, což v praxi nemusí být pro použití optimální.

Tabulka č. 4 zase zobrazuje, že v případě pořízení licence na dva roky je na tom DeepSucurity zcela jinak, než v předchozím případě.

15 Závěr

Hlavním cílem této bakalářské práce bylo zpracovat problematiku a přístupy HIPS (Host-based intrusion prevention system) na volně dostupná řešení, kde se měla provést výkonová a funkční komparativní analýza.

Následně byly popsány systémy detekce průniku (IDS) a systémy prevence průniku (IPS). Na základě popisu byly zohledněny výhody a nevýhody obou systémů a jejich rozdíly. K jejich popisu bylo nutné také představit jejich architekturu a komponenty, jelikož se jedná o klíčové pojmy.

Dále byly rozebrány konkrétní systémy detekce a prevence průniku (IDPS), mezi které patří NIDPS, WIDPS, NBA a HIPDS, a se kterými se následně pracovalo v praktické části.

K realizaci výkonové a funkční komparativní analýzy pro řešení HIPS byla vybrána tři dostupná řešení. Vybranými řešeními pro HIPS byly Comodo Internet Security Pro, ReHIPS a DeepSecurity. Tato řešení byla vybraná na základě typické odlišnosti mezi nimi samotnými. Všechna řešení byla v bakalářské práci legálně aplikovaná z volně z dostupných trial či demo verzí.

Komparativní analýza byla založena na porovnání v rámci poskytnutí funkcí a služeb daného HIPS řešení, uživatelské přívětivosti, jednoduchosti konfigurace, účinku při prevenci průniku, možnosti implementace a ceny pořízení konkrétního produktu.

Na výkonovou analýzu byl použit volně dostupný nástroj System Explorer, jehož cílem bylo sledovat vytížení procesoru (CPU), operační paměti (RAM) a swapovacího oddílu (SWP) na testovacím zařízení. Největší vliv na zátěž testovacího zařízení mělo řešení DeepSecurity, což je pochopitelné, pokud vezmeme v potaz, že se jednalo o nejobsáhlejší řešení ze všech.

Na závěr po provedení výkonové a funkční komparativní analýzy byla zhodnocena licenční politika v případě pořízení některého z vybraných produktů.

Seznam obrázků

Seznam tabulek

Seznam zkratek

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IDPS	Intrusion Detection Prevention System
HIPS	Host-based Intrusion Prevention System
HIDS	Host-based Intrusion DectionSystem
NBA	Network Behaviour Analysis
HIDPS	Host-based Intrusion Detection Prevention System
NIDPS	Network-based Intrusion Detection Prevention System
WIDPS	Wireless-based Intrusion Detection Prevention System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
NIC	Network Interface Controller
DMZ	Demilirated Zone
PC	Personal Computer
NB	Notebook
DDR	Double Data Rate
GB	Giga byte
MB	Mega byte
HD	High definition
CPU	Central Processing Unit
RAM	Random Access Memory
HDD	Hard Disc Drive
GPU	Graphic Processing Unit
GHz	Giga Hertz
MHz	Mega Hertz
DoS	Denial of service
DDoS	Distributed Denial of service
AP	Access Point

OS	Operating system (operační systém)
LAN	Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
AV	Antivirus
FW	Firewall
PRO	Professional
HTML	Hyper Text Markup Language
CD	Compact Disc
USB	Universal Serial Bus
ARP	Address Resolution Protocol
GUI	Graphic User Interface
DPC	Deferred Procedure Call
PID	ProcessIdentifier (process ID)
I/O	Input/Output
VM	Virtual Machine
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
POP3	Post Office Protocol
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name System
RPC	Remote Procedure Call
CLI	Command Line
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
SWP	Swap
COM	Communication port
ISO	International Organization for Standardization
OSI	Open Systems Interconnection

ISO/OSI	International Organization for Standardization/ Open Systems Interconnection
RPM	Revolutions Per Minute
SDRAM	Synchronous Dynamic Random Access Memory

Seznam použité literatury

[1] **ENDORF**, Carl F., Eugene. SCHULTZ a Jim. MELLANDER. Intrusion detection & prevention. New York: McGraw-Hill/Osborne, c2004. ISBN 0072229543

[2] **BEALE**, Jay, Andrew R. BAKER a Joel. ESLER. Snort: IDS and IPS toolkit. Burlington, MA: Syngress, c2007. ISBN 9781597490993

[3] **K. Scarfone**, P. Mell, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology (NIST), 2007

[4] **M. Azhagiri**, DrA. Rajesh and DrS. Karthik: Intrusion Detection and Prevention System: Technologies and Challenges, říjen 2015

[5] **Nicholas Pappas:** Network IDS & IPS Deployment Strategies, duben 2008. Dostupné z: https://www.sans.org/reading-room/whitepapers/intrusion/network-ids-ips-deployment-strategies-2143

[6] **Aaruni Goel**, Dr. Ashok Kumar Vasishtha: A Review on Foundation of Network Intrusion Detection and Prevention Systems (NIDPS), červen 2017. Dostupné z: http://www.csjournals.com/IJEE/PDF9-1/22.%20Aaruni.pdf

[7] **Michael E. Whitman**, Herbert J. Mattord, David Mackey a Andrew Green: Guide to Network Security. Boston: Cengage Learning, c2013. ISBN 978-0-8400-2422-0. Dostupné z: https://books.google.cz/books?id=VRQLAAAAQBAJ&pg=PA224&lpg=PA224&dq=net#v=onepage&q&f=false

[8] **Kopelo Letou**, Dhruwajita Devi, Y. Jayanta Singh: Host-based Intrusion Detection and Prevention System (HIDPS), květen 2013. Dostupné z: http://research.ijcaonline.org/volume69/number26/pxc3888419.pdf

[9] **Joel Scambray**, Stuart McClure, George Kurtz: Hacking Exposed: Network Security Secrets & Solutions. McGraw-HillCompanies, c2001. ISBN 80-7226-644-6.

[10] **Autor neznámý:** Softwarové firewally. Antivirové centrum. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[11] **Martin Kuchař:** Firewall – obraňte své počítače, únor 2005. Dostupné z: https://pctuning.tyden.cz/index.php?option=com_content&view=article&id=4296&catid=52&Itemid=78

[12] **Autor neznámý:** Počítačové viry. Gymnázium a Jazyková škola s právem státní jazykové zkoušky Zlín. Dostupné z: http://www.gjszlin.cz/ivt/esf/ostatni-sin/pocitacove-viry.php

[13] **Bc. Igor Hák:** Moderní počítačové viry, září 2005. Dostupné z: http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf

[14] **Bc. Jan Januš:** Problematika Host Intrusion Prevention System. Univerzita Pardubice Fakulta elektrotechniky a informatiky, květen 2015. Dostupné z: http://dspace.upce.cz/bitstream/handle/10195/61152/JanusJ_ProblematikaHost_JH_2015.pdf?sequence=1&isAllowed=y

[15] **Jonathan Chee:** Host Intrusion Prevention Systems and Beyond. SANS Institute, červen 2008. Dostupné z: https://www.sans.org/reading-room/whitepapers/intrusion/host-intrusion-prevention-systems-32824

[16] **Shahid Anwar**, Jasni Mohamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Suleman Khan, Bokolo Anthony a Victor Chang: From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements and Future Directions, březen 2017. Dostupné z: http://www.mdpi.com/1999-4893/10/2/39/htm

[17] **David Szep:** Detekce a analýza průniků systémy IDS a IPS. Jihočeská univerzita v Českých Budějovicích Přírodovědecká fakulta, 2013. Dostupné z: https://theses.cz/id/kwflec/Bakalsk_prce_-_Szep_David.pdf

[18] **Ken Hutchison:** Wireless Intrusion Detection Systems. SANS Institute, říjen 2004. Dostupné z: https://www.sans.org/reading-room/whitepapers/wireless/wireless-intrusion-detection-systems-1543

[19] **Dinesh Sequeira:** INTRUSION PREVENTION SYSTEMS – SECURITY'S SILVER BULLET?. SANS Institute, 2002. Dostupné z: https://www.sans.org/reading-room/whitepapers/detection/intrusion-prevention-systems-securitys-silver-bullet-366?show=366.php&cat=detection

[20] **Petr Bouška:** Počítačové sítě a jejich typy. Samuraj, červenec 2007. Dostupné z: https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/

[21] **Rafeeq Ur Rehman:** Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and ACID. New Jersey: PrenticeHall PTR, 2003. ISBN 0-13-140733-3

[22] **Burçin Gerçek:** Jak funguje antivirový program?. Symantec. Dostupné z: https://www.symantec.com/region/cz/resources/antivirus.html

[23] **Autor neznámý**: Počítačová bezpečnost (Computer security). Management mania, leden 2016. Dostupné z: https://managementmania.com/cs/pocitacova-bezpecnost

[23] **Autor neznámý:** DeepSecurity. Trend Micro. Dostupné z: https://www.trendmicro.com/en_ie/business/products/hybrid-cloud/deep-security-data-center.html

[24] **Autor neznámý:** DeepSecurity 9.6 Comprehensive security platform for physical, virtual, and cloudservers. Trend Micro. Dostupné z: https://www.trendmicro.com.hk/cloud-content/us/pdfs/business/datasheets/ds_deep-security.pdf

[25] **Jan Kejda:** Integrace IDS/IPS systému na bázi open source a komerčních technologií. Mendelova univerzita v Brně Provozně ekonomický fakulta, 2010. Dostupné z: https://is.mendelu.cz/lide/clovek.pl?zalozka=13;id=398;studium=31149;zp=27673;download_prace=1;lang=cz

[26] **Bc. Michal Černý:** Systémy detekce a prevence průniku. Vysoké učení technické v Brně fakulta elektrotechniky a komunikačních technologií ústav telekomunikací, 2010. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=27248

[27] **Autor neznámý:** ReHIPS Review. My Digital Life, únor 2018. Dostupné z: https://forums.mydigitallife.net/threads/written-review-rehips-review.76365/

[28] **Bc. Zdeněk Kugler:** Proxy Firewall. Vysoké učení technické v Brně fakulta elektrotechniky a komunikačních technologií ústav telekomunikací, 2009. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=15131

[29] **Autor neznámý:** Intrusion Detection Systems. Durofy, listopad 2013. Dostupné z: http://durofy.com/intrution-detection-system/

[30] **Miroslav Čermák:** Co je to HIDS/HIPS a k čemu slouží. Clever and Smart, listopad 2014. Dostupné z: https://www.cleverandsmart.cz/co-je-to-hidships-a-k-cemu-slouzi/

[31] **Autor neznámý:** What Is a Proxy Server and How Does It Work. Top Ten Reviews. Dostupné z: https://www.toptenreviews.com/software/articles/what-is-a-proxy-server-and-how-does-it-work/

[32] **Autor neznámý:** HIPS Settings. Comodo. Dostupné z: https://help.comodo.com/topic-72-1-623-7731-.html

[33] **Margaret Rouse:** proxy server. Techtarget, leden 2015. Dostupné z: https://whatis.techtarget.com/definition/proxy-server

[34] **Autor neznámý:** What is a proxy server?. IPLocation. Dostupné z: https://www.iplocation.net/proxy-server

[35] **Autor neznámý:** What is a denial of service attack (DoS)?. Palo Alto Networks. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[36] **Autor neznámý:** Denial of service attacks chat you need to know. CERT UK, 2014. Dostupné z: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Denial-of-service-attacks-what-you-need-to-know1.pdf?platform=hootsuite

[37] **Autor neznámý:** Guideline on Intrusion Detection and Prevention Systems. National Computer Board, říjen 2011. Dostupné z: http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Intrusion%20Detection%20and%20Prevention%20Systems.pdf

[38] **Autor neznámý:** Host-based intrusion prevention system (HIPS). Techopedia. Dostupné z: https://www.techopedia.com/definition/4290/host-based-intrusion-prevention-system-hips

[39] **Pieter Arntz:** What is Host Intrusion Prevention System (HIPS) and how does it work?. Malwarebytes LABS, květen 2013. Dostupné z: https://blog.malwarebytes.com/101/2013/05/whatiships/

[40] **Autor neznámý:** HIPS Explained. Gizmo's freeware, květen 2016. Dostupné z: https://www.techsupportalert.com/content/hips-explained.htm

[41] **B. Santos Kumar**, T. Chandra Sekhara Phani Raju, M. Ratnakar, Sk. Dawood Baba a N. Sudhakar: Intrusion Detection System - Types and Prevention. International Journal of Computer Science and Information Technologies, 2013. Dostupné z: http://ijcsit.com/docs/Volume%204/Vol4Issue1/ijcsit2013040119.pdf

Přílohy

Přílohy obsahují odkazy ke stažení softwaru, který byl aplikován pro praktickou část bakalářské práce.

1) ReHIPS 2.4.0 Demo verze
   https://rehips.com/en/

2) Trend MicroDeepSecurity 9.6 Trial verze
   https://www.trendmicro.com/product_trials/download/index/us/123

3) COMODO Internet Security Pro 11 Trial verze
   https://www.comodo.com/home/download/during-download.php?prod=cispro8&track=1150&ref=TDJodmJXVXZhVzUwWlhKdVpYUXRjMlZqZFhKcGRIa3ZhVzUwWlhKdVpYUXRjMlZqZFhKcGRIa3RjSEp2TG5Cb2NBPT0=

4) System Explorer 7.0.0.5356 freeware verze
   http://systemexplorer.net/

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Horáček Jonáš	Pod Haltýřem 259, Hradec Králové - Svinary	I1700515

TÉMA ČESKY:

Komparativní analýza řešení HIPS

TÉMA ANGLICKY:

Comparative analysis of HIPS solution

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce zpracovat problematiku HIPS z pohledu výkonové analýzy zaměřené na volně dostupná řešení. Autor práce podrobně představí problematiku a přístupy řešení HIPS. Na základě provedené analýzy vybere relevantní volně dostupná řešení a provede jejich výkonovou a funkční komparativní analýzu.V rámci analýzy autor zohlední nároky řešení HIPS na systémové zdroje a případné ekonomické dopady jeho implementace.

Osnova práce:
Úvod
Rešerše problematiky
Představení principů HIPS
Analýza dostupných řešení HIPS
Stanovení výchozích hypotéz
Stanovení metodiky pro komparativní analýzu
Komparativní analýza vybraných řešení
Vyhodnocení hypotéz
Závěr

SEZNAM DOPORUČENÉ LITERATURY:

ENDORF, Carl F., Eugene. SCHULTZ a Jim. MELLANDER. Intrusion detection & prevention. New York: McGraw-Hill/Osborne, c2004. ISBN 0072229543.

BEALE, Jay, Andrew R. BAKER a Joel. ESLER. Snort: IDS and IPS toolkit. Burlington, MA: Syngress, c2007. ISBN 9781597490993.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....