Nasazení bezpečnostního nástroje Eset Protect ve firemním doménovém prostředí

Josef Novák

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Josef Novák**
Osobní číslo:	**A18131**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Nasazení bezpečnostního nástroje Eset Protect ve firemním doménovém prostředí**
Téma práce anglicky:	**Deployment of the Eset Protect Security Tool in a Corporate Domain Environment**

Zásady pro vypracování

1. Zpracujte literární rešerši zaměřenou na téma bezpečnostního řešení a správu koncových zařízení v doménovém prostředí.
2. Proveďte porovnání nejpoužívanějších řešení a srovnání jejich funkčnosti.
3. Popište proces nasazení a výchozího nastavení nástroje Eset Protect.
4. Otestujte funkčnost bezpečnostního řešení Eset Protect a popište postup řešení nejběžnějších událostí, které mohou nastat.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. STANEK, William R. Microsoft Windows Server 2012: kapesní rádce administrátora. Přeložil Jiří HUF. Brno: Computer Press, 2015. ISBN 9788025138175.
2. HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 9788025131763.
3. STANEK, William R. Group Policy: zásady skupiny ve Windows: kapesní rádce administrátora. Brno: Computer Press, 2010. ISBN 9788025129203.
4. MERHAUT, Filip a Ivan ZELINKA. Počítačové viry a bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008 [i.e. 2009]. ISBN 9788073187637.
5. LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 9788025146026.
6. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 8025101061.

Vedoucí bakalářské práce: **Ing. David Šaur, PhD.**
Ústav matematiky

Datum zadání bakalářské práce: **17. ledna 2022**
Termín odevzdání bakalářské práce: **31. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 17. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 24.5.2022

Josef Novák, v .r.
podpis studenta

ABSTRAKT

Práce se zabývá nasazením bezpečnostního balíčku od firmy Eset včetně vzdáleného managementu a jeho implementaci v typickém firemním prostředí. V teoretické části práce jsou popsány a vysvětleny základní pojmy doménového firemního prostředí, virtualizace, počítačové bezpečnosti, nejčastějších počítačových hrozeb a v neposlední řadě porovnání bezpečnostních balíčků od několika firem. V praktické časti práce jsou nejprve popsány jednotlivé části testovacího prostředí, pod kterým byl produkt firmy Eset testován. Následně postup jeho nasazení včetně základního nastavení. A na závěr práce jsou demonstrovány různé možnosti použití nástroje Eset Protect.

Klíčová slova: počítačová bezpečnost, antivirus, Eset

ABSTRACT

The thesis deals with the deployment of the Eset security package including remote management and its deployment in a domain company environment. The theoretical part of the thesis describes and explains basic concepts of the domain corporate environment, virtualization, computer security, common computer threats and last but not least a comparison of security packages from several companies. The practical part of the thesis firstly describes the different parts of the test environment under which the Eset product was tested. Afterwards, a description of its deployment is given, including its basic setup. Finally, the various possibilities of using Eset Protect are demonstrated.

Keywords: computer security, antivirus, Eset

Rád bych zde poděkoval vedoucímu práce panu Ing. Davidu Šaurovi, Ph.D., za odborné vedení, rady a zpětnou vazbu při zpracovávání bakalářské práce. Dále chci poděkovat rodině a kamarádům za podporu během studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době je pojem počítačová bezpečnost velmi frekventované téma, které do budoucna bude stále důležitější a komplexnější. Rok od roku se potkáváme s novými a stále složitěji odhalitelnými počítačovými hrozbami a je potřeba na ně adekvátně reagovat. Firmy ročně vynakládají stále více prostředků na obranu proti různým ransomwarům, phishingu apod. Školí uživatele, nasazují modernější nástroje a řeší sofistikovanější zálohy svých dat.

V této práci jsem se konkrétně zaměřil na problematiku bezpečnosti koncových uživatelských stanic na systému Microsoftu a v typickém firemním prostředí s Active Directory.

Bakalářská práce je rozdělena na teoretickou a praktickou část. V teoretické části jsou vysvětleny pojmy spojené s firemním doménovým prostředím a virtualizací. Dále je tato část zaměřena na počítačovou bezpečnost. Jsou zde uvedeny typy útoku, podvodné techniky, které jsou útočníky využívány a možnosti ochrany koncových zařízení. Zakončení této části obsahuje popis vybraného bezpečnostního balíčku od firmy Eset. Jsou zde rozebrány jednotlivé části bezpečnostního balíčku, hardwarové požadavky a porovnání s bezpečnostními balíčky od konkurenčních firem.

Praktická část se zabývá samotnou implementací bezpečnostního balíčku a jeho následnou konfigurací. V úvodu praktické části jsou vysvětleny jednotlivé části testovacího prostředí, jež bylo připraveno pro účel nasazení a také testování bezpečnostního balíčku. Testovací prostředí bylo vytvořeno jako náhrada firemního doménového prostředí, pro které bezpečnostní balíček slouží. Dále se praktická část zaměřuje na instalaci bezpečnostního balíčku ve virtuálním prostředí a jeho prvotní konfiguraci. Závěrečná část je věnována testování funkčnosti nainstalovaného bezpečnostního balíčku a jsou zároveň otestovány nejběžnější scénáře využitelné v praxi.

Bakalářská práce může sloužit pro majitele firem při výběru bezpečnostního řešení. A také jako ukázka konkrétního bezpečnostního balíčku od firmy Eset.

I. TEORETICKÁ ČÁST

1 DOMÉNOVÉ PROSTŘEDÍ

Doménové prostředí založené na Active Directory a dalších pomocných službách, jako jsou DNS, DHCP nebo například AD DS, nám umožnuje řešit centralizovaně správu jednotlivých uživatelů, počítačů, tiskáren atd. v rámci firem všech velikostí.

Centrální správa jednotlivých zařízení nám usnadňuje nastavování práv pro jednotlivé prostředky, jako jsou oprávnění k přístupu k souborům či složkám na souborovém serveru, umožňuje jednotné přihlašování do různých systémů a zařízení ve firmě apod.

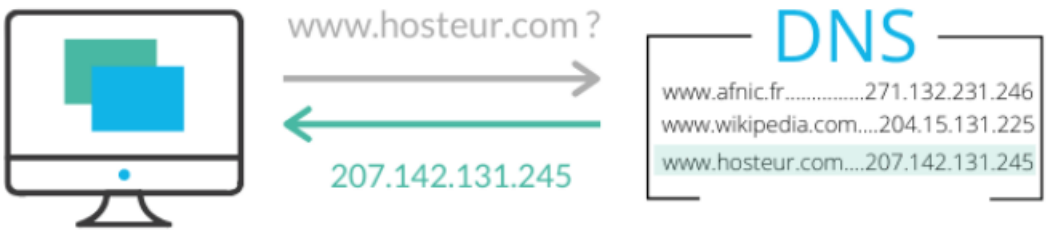
V následující kapitole budou blíže popsány jednotlivé komponenty a služby.

1.1 Domain Name System (DNS)

DNS se rozumí taková služba, jenž převádí názvy počítačů na IP adresy. V případě vytvoření reverzního DNS záznamu lze provést převod i naopak. DNS služba využívá ke své funkci zásobník protokolů TCP/IP.

Pomocí DNS sestavujeme skupiny počítačů do domén. Domény jsou organizovány v hierarchické struktuře. Dělíme je do kategorií, nejvyšší stupeň hierarchie tvoří domény nejvyšší úrovně.

DNS server je jedním se základních prvků infrastruktury každé firmy či poskytovatele internetového připojení. 62[1]



Obrázek 1. Ukázka funkce DNS [4]

1.2 Dynamic Host Configuration Protocol (DHCP)

Díky protokolu DHCP můžeme centralizovaně řídit přidělování IP adres. DHCP má svůj účel i v další oblasti správy. Pomocí DHCP serveru můžeme síťovým kartám, které se nachází v počítači, přiřazovat dynamické IPv4 nebo IPv6 adresy.

Počítač, kterému je dynamicky přidělena IPv4 adresa se nazývá DHCPv4 klientem. Po spuštění klient obdrží 32bitovou IPv4 adresu. Adresa je vybrána z fondu IPv4 adres definovaných na DHCP serveru. Tato adresa je klientovi přidělena na určitou dobu. Po uplynutí poloviny doby se klient pokusí výpůjčku obnovit. V případě, že nebude možné o IP adresu zažádat po uplynutí poloviny období zápůjčky, klient se o to pokusí těsně před vypršením doby zápůjčky. [1] [2]

Obrázek 2. Ukázka funkce DHCP [5]

1.3 Active Directory (AD)

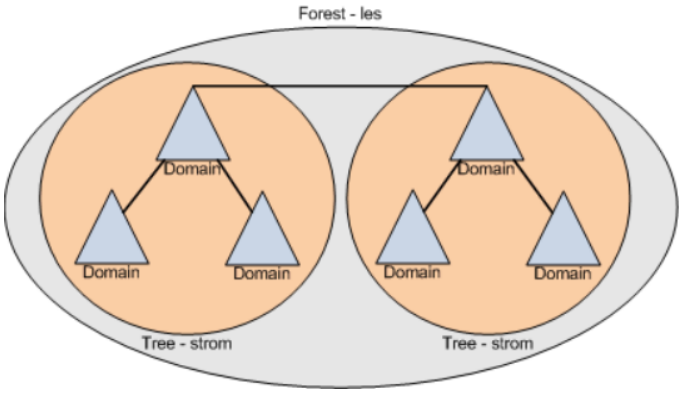
Služba pro správu firemní počítačové sítě. Primární rolí AD je poskytování centrálních služeb pro autentizaci a autorizaci. AD obsahuje mnoho dalších funkcí, jako například Group Policy. AD je silně provázáno s DNS a používá stejnou strukturu. Uložená data jsou organizována ve formě objektů. [6]

1.3.1 Schéma AD

K vytvoření struktury adresáře slouží jednotlivé komponenty. Struktura adresáře je tvořena tak, aby odpovídala struktuře firmy a splňovala její požadavky. Komponenty zastupují

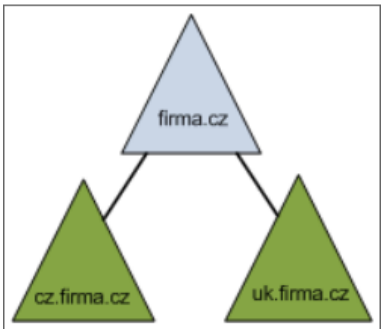
logickou nebo fyzickou strukturu. Logickou strukturu v AD vytvoříme pomocí topologické struktury[1] Active Directory. Na vrcholu logické struktury se nachází les.

Les – je tvořen jedním nebo více oddělenými stromy. Každý strom v lese má vlastní pojmenování. Domény v lese pracují nezávisle, sdílí stejné schéma a jsou propojeny implicitním vztahem. [6]



Obrázek 3. Ukázka schéma AD les [6]

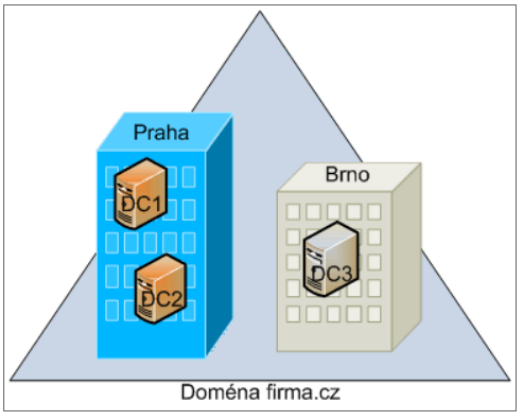
Strom – je hierarchická organizace nebo seskupení jedné či více domén. K vytvoření stromu se používá kořenová doména, ke které přidáme podřízenou doménu. Domény sdílí souvislý jmenný prostor. K vytváření používáme DNS standard.



Obrázek 4. Ukázka schéma AD strom [6]

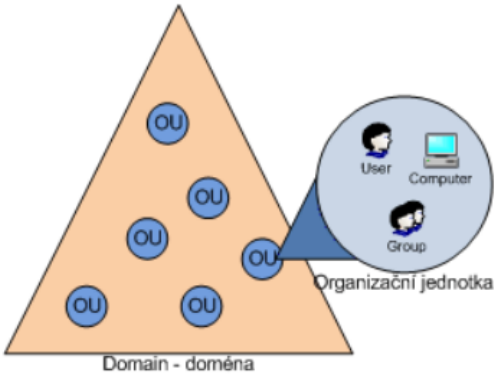
[1] Topologická struktura Active Directory se vytváří pomocí lesa, stromů, domén a organizačních jednotek. Používá se k vytvoření struktury adresáře. Komponenty v topologii Active Directory zastupuji logickou strukturu společnosti.[6]

Doména – je základem logické struktury AD. Nachází se zde uložené objekty, které k dané doméně náleží. Počet objektů v doméně není omezen. Active Directory může tvořit jedna nebo více domén. Přístup k jednotlivým objektům domény je řízen pomocí ACL. [6]



Obrázek 5. Ukázka schéma AD doména [6]

Organizační jednotky (OU) – jsou nejmenší jednotky, na které lze delegovat administrační oprávnění. Jedná se o kontejner pro organizování objektů do administračních skupin. Z organizačních jednotek můžeme vytvářet libovolnou hierarchickou strukturu. [6]



Obrázek 6. Ukázka schéma AD organizační jednotka [6]

1.3.2 Active Directory Certifikate Services (AD CS)

Pomocí AD CS spravujeme digitální certifikáty uživatelů, klientů a serverů. Tato služba využívá certifikační autority, nesoucí zodpovědnost za ověřování identity uživatelů a počítačů. Vydává certifikáty, které jejich identitu potvrzují. Domény využívají kořenové firemní certifikační autority, jenž tvoří certifikační servery. Tyto certifikační servery se nalézají na kořenové certifikační hierarchii domén. Dále mohou být využívány nejdůvěryhodnější firemní certifikační servery a podřízené certifikační autority, jež jsou

členy konkrétní firemní certifikační hierarchie. Pracovní skupiny využívají své vlastní kořenové certifikační autority. Využívají také certifikační autority, které jsou členy nefiremní certifikační hierarchie. [1]

1.3.3 Active Directory Domain Services (AD DS)

Pomoci AD DS zajištujeme základní adresářové služby. Tyto služby jsou potřebné k založení domény a datového úložiště, jenž má za úkol uchování informací o objektech v síti a tyto informace zpřístupní uživatelům. Pro službu AD DS se využívá řadičů domény. Po přihlášení uživatelů do domény a následnému ověření, dojde k uložení přihlašovacích údajů. Uložené přihlašovací údaje je možné použít k přístupu k zdrojům v síti. [1]

1.4 Group Policy Object (GPO)

Skupinové politiky se používají pro centrální správu počítačů za pomoci Active Directory. Jedná se o virtuální kolekci nastavení zásad. GPO má jedinečný název a může reprezentovat nastavení zásad v systému souborů a ve službě Active Directory. Nastavení GPO je vyhodnocováno pomocí Active Directory. Zavedení zásad probíhá při spuštění počítače a přihlášení uživatele. Při zapnutí počítače uživatelem dojde k zavedení zásad počítače. Po přihlášení uživatele dojde k načtení profilu uživatele a zavedení zásad uživatele. [7] [8]

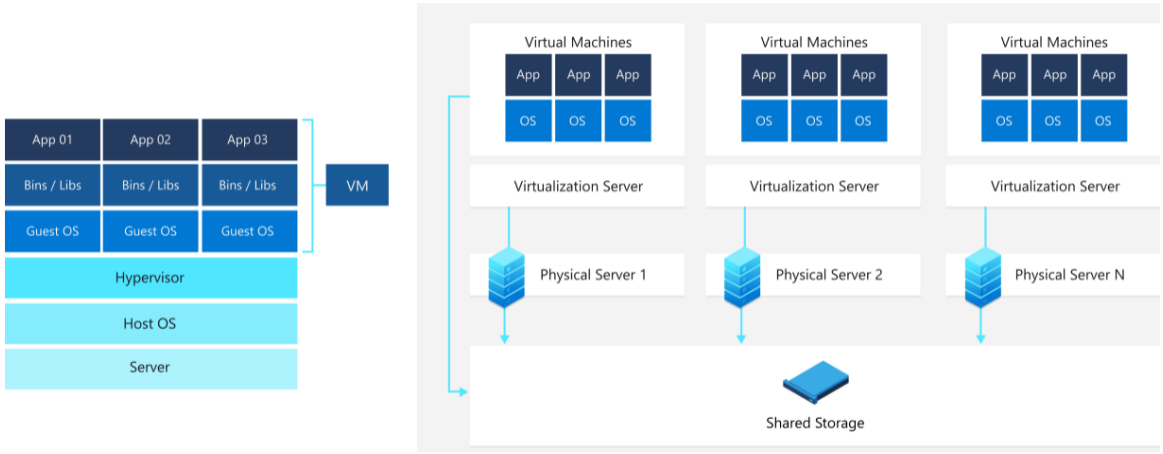
1.5 Virtualizace

Virtualizaci používáme k vytvoření simulovaného nebo virtuálního výpočetního prostředí. Toto vytvořené prostředí využíváme namísto fyzického prostředí. Díky virtualizaci můžeme rozdělit jeden počítač nebo server na několik virtuálních počítačů, kde je každý takový virtuální počítač schopen pracovat nezávisle. Virtualizace dopomáhá ke snížení spotřeby energie, nákladů na infrastrukturu a snížení počtu využívaných serverů.

Virtualizaci můžeme rozdělit do čtyř hlavních kategorií. První kategorií se nazývá virtualizace plochy a umožnuje jednomu centralizovanému serveru poskytovat či spravovat přizpůsobené plochy. Druhou kategorií je virtualizace sítě, využitelná k rozdělení šířky pásma sítě. Šírku pásma rozdělíme mezi nezávislé kanály. Tyto kanály se přiřadí konkrétním serverům nebo zařízením. Třetí kategorií je virtualizace softwaru a využívá se k oddělení aplikací od hardwaru a operačního systému. Poslední čtvrtou kategorií je virtualizace úložiště, kombinující prostředky síťového úložiště v jednom úložném zařízení. K tomuto zařízení má přístup více uživatelů.

1.5.1 Hypervisory

Jsou základním prvkem virtualizace, oddělující fyzický hardware od virtuálního. Hypervisory vytváří vlastní virtualizační vrstvu. Jejich úkolem je přerozdělování zdrojů hostitele. Mezi tyto zdroje řadíme operační systém, procesor a disk, tak aby byly v potřebné míře k dispozici pro virtuální počítač. Dalším využitím je zajištění komunikace mezi fyzickým a virtuálním hardwarem. Hypervisory mají své dělení, a to na hostované a nativní. Hostované hypervisory jsou spuštěny na běžícím operačním systému. Nativní hypervisory jsou používány pro virtualizaci serverů. Rychlost a stabilita virtuální počítačů je ovlivněna kvalitou hypervisoru.



Obrázek 7. zobrazení schéma hostovaného a nativního hypervisoru [11]

1.6 Závěrečné shrnutí

První kapitola teoretické části je věnována seznámení se s doménovým prostředím a jeho jednotlivými základními prvky. Jsou zde vysvětleny pojmy jako DNS, DHCP a Active Directory. Dále je zde zmíněn význam skupinových politik a pojem virtualizace.

2 POČÍTAČOVÁ BEZPEČNOST

Počítačová bezpečnost je zaměřena na bezpečnost informačních a komunikačních technologií. Je bezpochyby zřejmé, že se jedná o důležitou součást informační bezpečnosti. Počítačová bezpečnost se týká nejen koncových zařízení, ale také všech dalších částí IT infrastruktury. Cílem je zamezení počítačovým útokům a zajištění bezpečného provozu zařízení. Počítačová bezpečnost je realizována pomocí bezpečnostního softwaru i pomocí hardwarových opatření. V podnicích je realizována IT specialistou. Kapitola se věnuje popisu kybernetických útoků. [13]

2.1 Škodlivý software – malware

Mezi škodlivý software řadíme druhy programů, které škodí uživateli. Hlavním úkolem škodlivého softwaru je poškození dat uživatele. Co se týče samotného názvu, můžeme se setkat i s anglickým označením malware. Mezi nejznámější škodlivý software patří počítačový virus. Dalším škodlivý software je počítačový červ, který se vyznačuje zejména možností šíření pomocí počítačové sítě. K dalším druhům škodlivého softwaru patří trojští koně, spyware, adware, ransomeware, keylogery a další. V dnešní domě se pro zisk informací používají techniky phishing, farming a sociální inženýrství.

Odhalení infikování malwarem je v dnešní době pro běžného uživatele značně obtížné. Dříve se jako typické příznaky uváděly obecné snížení výkonu, zpomalení přístupu k internetu, pády programů a neobvyklé chování počítače. V současnosti počítače disponují vysokým množstvím výkonu a rychlost internetového připojení je na vysoké úrovni. Z toho plyne že běžný uživatel není schopen příznaky napadení rozpoznat. Jediným pozorovatelným příznakem zůstávají neobvyklé chování a pády aplikací. [3] [14]

2.1.1 Počítačový virus

Počítačový virus využívá ke svému šíření hostitele, kdy je ve většině případů je virus vložen do těla spustitelného souboru, který obsahuje část spustitelného kódu. Infikované soubory jsou následně využívány jako prostředky pro šíření viru a napadení dalších zařízení. Zmíněný typ počítačového viru označujeme jako souborové viry.

Druhou skupinou jsou viry, které ke svému šíření využívají boot sektory. Virus obsažen v boot sektoru je zaveden do počítače ihned po spuštění. Zavedení proběhne dříve, než je

zaveden operační systém a antivirová ochrana. Tento druh se hojně používal v minulosti, kdy byly pro bootování používány bootovací diskety.

Jakožto speciální skupinu můžeme označit makro viry. Jedná se o makra, která se samovolně kopírují a šíří se zejména v kancelářských dokumentech. V dnešní době se již viry ve velké míře neobjevují, jelikož programy pro spouštění maker obsahují ochranu proti samo spouštění. [3] [15] [16]

2.1.2 Počítačový červ

Jedná se o druh škodlivého programu, který ke svému šíření nepotřebuje hostitelský soubor. Počítačový červ se sám aktivně šíří po počítačové síti a k této činnosti využívají bezpečnostních děr v operačním systému. Po aktivaci počítačového červa může dojít k mazaní souborů, zpomalení činnosti a deaktivaci programů. Díky vysokému rozšíření internetu je možné rozšíření počítačového červa po celém světě během několika hodin. Počítačový červ může být využit k dalším infiltracím do systému. Počítačové červy můžeme rozdělit na několik typů, a to emailový červ, internetový červ, IM IRC červ a červ využívající sdíleného prostoru.

Jak už z názvu vyplývá, emailový červ využívá ke svému šíření emailové klienty. Přes elektronickou poštu je poslána infikovaná příloha, kterou uživatel otevře. Po napadení nového počítače se začne šířit pomocí emailových adres, které získal z adresáře oběti.

Internetoví červi se rozšiřuje pomocí počítačové sítě, kde skenují počítače v síti a v situaci nalezení zranitelného počítače, využijí zranitelnosti a provedou útok. Při efektivním využití zranitelnosti červem je infikování možné provést bez vědomí uživatele.

IM a IRC červ se rozšiřuje v síti pro komunikaci v reálném čase. IM červ útočí pomocí rozesílaní odkazů na nebezpečné stránky, přes které dojde k infikování počítače. IRC červi využívají k útoku zasílání programu jako spustitelného souboru. IRC červi jsou méně nebezpeční, jelikož k infikování dojde až po stáhnutí a spuštění souboru.

Poslední varianta využívá ke svému šířeni kopie svého programu uloženého jako spustitelný soubor. Tento soubor je uložený na sdíleném prostoru lokálního počítače a je možné ho stáhnout. Po stažení a spuštění je provedena infikace počítače. [3] [17] [18]

2.1.3 Trojský kůň

Název trojský kůň je odvozen od starořecké pověsti o dobytí Tróji. V dnešní době se tento název využívá pro škodlivý software, který je schován v jiných programech nebo souborech. Tyto programy vypadají jako užitečné a vybízí ke spuštění uživatelem. Trojský kůň může být využit na otevírání zadních vrátek, převzetí kontroly nad napadeným počítačem, pro získání uživatelských dat a následné odeslání útočníkovi nebo pro stažení a spuštění jiného škodlivého softwaru. Narozdíl od virů, u trojského koně nedochází k infikaci dalších souborů. Po detekci trojského koně je doporučené daný soubor odstranit. Trojské koně můžeme dělit do několika kategorií. Dále jsou vypsány neznámější z nich.

Downloader – program sloužící k stahování dalšího škodlivého softwaru z internetu.

Dropper – program, který obsahuje ukrytý škodlivý software a přenáší jej. Dochází ke stižení detekce hrozby antivirovou ochranou.

Backdoor – umožňuje komunikaci se vzdáleným útočníkem. Dopomáhá útočníkovi k získání přístupu a přebrání kontroly nad napadeným systémem.

Keylogger – program pro sledování stisku kláves. Zjištěné údaje jsou poslány útočníkovi. Slouží pro zisk přihlašovacích údajů. [19] [20]

2.1.4 Spyware

Jde o těžce odhalitelný škodlivý software, jelikož se programy typu spyware instalují na pozadí a jejich chování v systému je velmi nenápadné. Činnost je maskována za důvěryhodné procesy. Hlavním cílem programů je odesílaní informací o uživateli bez jeho vědomí. Odesílány mohou být seznamy navštívených stránek, adresář emailových kontaktů a další. Data získaná pomocí spyware programů mohou obsahovat citlivá data, jako například bankovní účty a bezpečnostní kódy.

Šíření spyware probíhá s volně dostupnými programy. Autoři programů odůvodňují sběr dat tím, že jsou používána pro účel zobrazování cílené reklamy. Ovšem hranice zneužitelnosti dat je velmi tenká. [21] [22]

2.1.5 Ransomware

Škodlivý kód, který zamyká přístup k napadenému zařízení nebo šifruje data v zařízení. Tento druh programu se používá k vydírání napadených uživatelů. V případě napadení pomocí ransomware dojde k zobrazení zprávy s požadavkem o zaplacení určité částky.

V případě nezaplacení uvedené částky, může dojít k zvýšení ceny nebo se zařízení stane neovladatelné. Částka je ve většině případů uváděna v Bitcoinech nebo jiných kryptoměnách. Výhodou požadovaní platby kryptoměnou je, že je těžce do sledovatelná. Po zaplacení částky by mělo být zařízení odemknuto.

Ransomware může fungovat několika způsoby. Buďto se jedná o diskcoder, ten po napadení šifruje pevný disk a brání vstupu do operačního systému. Dalším je Screenlocker blokující uživateli přístup na obrazovku zařízení. A nakonec Crypto ransomware šifrující data uložená na disku.

Ochrana proti ransomware zajišťuje kvalitní bezpečnostní řešení, pravidelná záloha dat a pravidelná aktualizace aplikací včetně operačního systému. [23] [24] [25]

2.1.6 Adware

Hlavní úlohou adware je zobrazovaní reklam, přičemž se jedná o reklamy ve vyskakovacích oknech, webových stránkách nebo reklamy překrývající část obrazovky. Samotný adware není nijak škodlivý, jenom znesnadňuje práci na PC, nicméně reklama může odkazovat na phishingové stránky nebo stránky šířící jiný druh malwaru. Adware je hojně používán výrobci volně šiřitelných programů. Výdělek z reklam používají pro další vývoj aplikace. [26] [27] [28]

2.2 Podvodné techniky

2.2.1 Phishing

Při phishingovém útoku se útočníci vydávají za důvěryhodnou organizaci s cílem získat citlivá data od oběti útoku. Nejčastěji se útočníci pokoušejí získat přihlašovací údaje, hesla, informace o kreditní kartě a internetovém bankovnictví. Princip útoku je založen na rozesílaní podvodných emailů, kde se obvykle nachází link, který oběť přesměruje na podvodné stránky, vyžadujíc vložení citlivých údajů. Tyto stránky jsou vedeny ve stejném stylu jako oficiální stránky organizace. Údaje jsou následně útočníkem zneužity. Nejúčinnější obranou proti phishingovým útokům je školení koncových uživatelů. [29] [30]

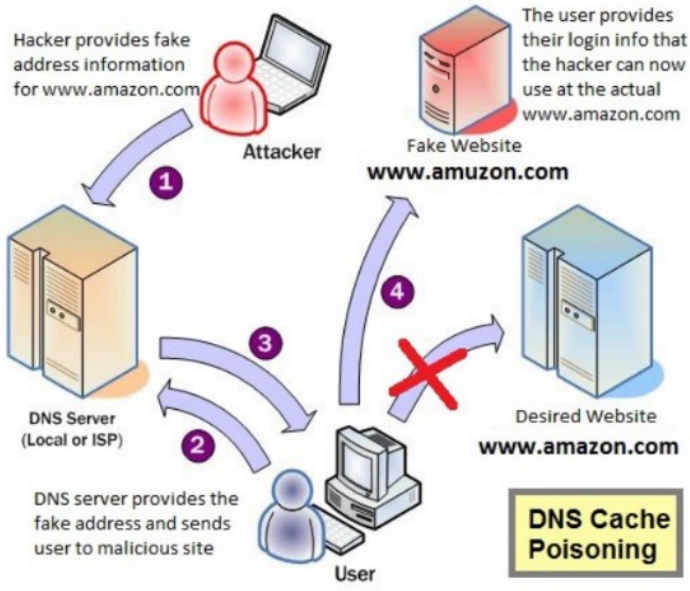
2.2.2 Pharming

Pharming je typ útoku využívající sociálního inženýrství, s cílem zisku citlivých osobních údajů, jako přihlašovacích jmen, hesel, údajů o kreditní katě a dalších nebo instalace

škodlivého softwaru. Útočníci přesměrovávají oběť na podvodnou stránku, která vypadá jako stránka, na kterou se uživatel chtěl připojit. Nejčastěji jsou vytvářeny falešné stránky bank a internetových obchodů.

Při útoku pharmingem je zneužíváno základu procházení internetu, a to tak, že internetová adresa musí být serverem DNS přeložena na IP adresu pro pokračování připojení. Pharming se provádí dvěma způsoby.

Při prvním způsobu útočník pomocí elektronické pošty odešle škodlivý software, přičemž k rozeslání škodlivého softwaru jsou používány phishingové techniky. Tento škodlivý software přepíše soubor místních hostitelů, který odkazuje na adresář IP adres a názvů domén. Tímto způsobem se přesměruje provoz ze zamýšlené webové stránky na stránky podvodné. Díky přepsání souboru host dojde k přesměrování vždy i po zadaní správné internetové adresy.



Obrázek 8. Schéma útoku pomocí pharming [47]

Při druhé metodě útočníci napadají DNS server, kde mohou modifikovat tabulky v DNS serveru. Při použití této varianty útoku je schopno podvodné stránky navštívit vyšší množství obětí. Po přesměrování na podvodnou stránku dochází ke sběru citlivých dat a je možnost instalace škodlivého softwaru. Útok na DNS servery je náročnější, ale profit útočníků je vyšší. Může dojít i k napadení dalších DNS serverů. Tento druh útoku je velmi nebezpečný, neboť může postihnut i uživatele, kteří mají počítač zcela bez škodlivého softwaru.

Jako ochrana proti napadení pharmingem může sloužit výběr důvěryhodného poskytovatele internetových služeb. Takový poskytovatel filtruje podezřelá přesměrování a díky tomu je menší šance na přesměrování na podvodnou stránku. Další možností je použití spolehlivého DNS serveru nebo je dále možné přejít na specializované DNS služby. V neposlední řadě je to kontrola stránek, zda mají platný bezpečnostní certifikát a kontrola internetových adres, zda se v nich nenacházejí překlepy. Samozřejmostí je nainstalování kvalitního antivirového programu s ochranou proti malware. [31] [32]

2.3 Bezpečnostní software

2.3.1 Antivirový program

V dnešní době antivirové programy obsahují řadu bezpečnostních vrstev a disponují moderními technologiemi. Takový typ řešení chrání uživatele před nejrůznějšími hrozbami. Dříve se jednalo o jednoduchý software pro detekci a odstranění počítačového viru. Antivirové programy můžeme rozdělit podle způsobů jakými vir vyhledávají. Nejstarším řešením je vyhledávaní pomocí signatur, spočívající ve skutečnosti, že každý virus obsahuje unikátní řetězec (signaturu), podle něhož je možné jednoznačné určení. Signatury jsou uloženy v databázi signatur. Databázi je nutné šifrovat z důvodu eliminace falešných poplachů je nutné, aby byla udržována v aktuálním stavu.

Dalším způsobem je vyhledávání na základě heuristické analýzy. Tento typ detekce by měl odhalit i viry, pro které nebyly doposud vytvořeny signatury. Základem je vyhledání podezřelých projevů programu, které jsou typické pro počítačový virus. Jednou z nevýhod je nemožnost pojmenovat virus. Ve většině případů je heuristická analýza kombinována s testem signatur. [3] [33]

2.4 Firewall

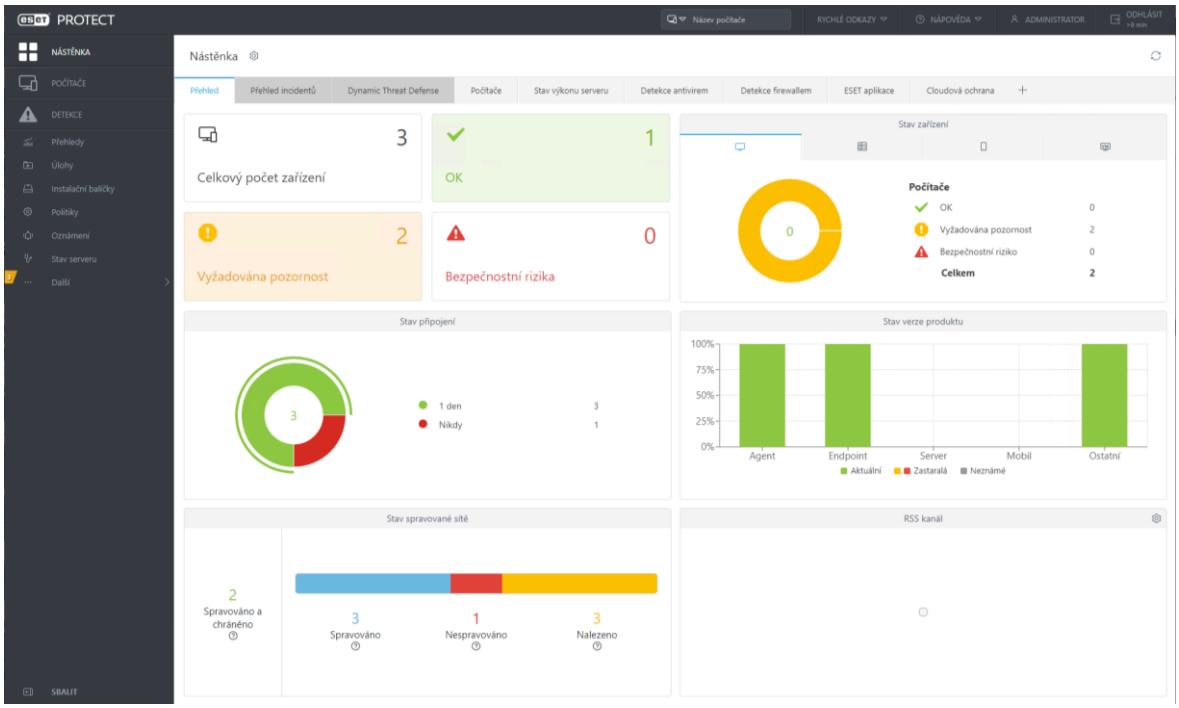
První článek obrany sítě před útoky z vnějšku, jenž zajišťuje blokování nebo povolování navazované komunikace na základě pravidel a politik. Firewall může být jak softwarový, tak hardwarový. Firewall chrání zařízení, která jsou zapojena za ním. Rozdělení firewallu je do dvou základních skupin, a to síťový firewall a personální. [3] [34]

2.5 Závěrečné shrnutí

Kapitola je zaměřena na počítačovou bezpečnost. Jsou zde uvedeny nejčastější kybernetické hrozby, které mohou postihnout kteréhokoli uživatele počítačové techniky. Dále je zde popsána obrana proti těmto hrozbám v podobě antivirového programu, který je již nedílnou součástí všech zařízení a firewallu.

3 ESET PROTECT

Eset Protect je nástroj pro správu produktů od společnosti Eset. Umožňuje jednotnou správu bezpečnostních produktů na stanicích, serverech i mobilních zařízení. Správa je prováděna z jednoho centrálního místa v síti. Je vhodný pro vzdálenou instalaci bezpečnostních řešení a konfiguraci. [35]



Obrázek 9. Náhled prostředí Eset Protect

3.1 Komponenty

Nástroj Eset Protect se skládá z dále popsaných komponent:

- **Eset Protect Server** – slouží k uchovávání dat v databázi a zajišťuje komunikaci s klientskými stanicemi. Vhodný pro instalaci na Windows, Linux nebo virtuálního prostředí.
- **Eset Protect Web Console** – webové rozhraní pro správu počítačů v síti. Umožnuje vzdálené nasazení bezpečnostních produktů a poskytuje přehled o všech klientech v síti. Nasazení je možné i na zařízení, které není pod správou Eset Protect Web Console.
- **Eset Protect Management Agent** – zprostředkovává komunikaci mezi klientskou stanicí a Eset Protect Serverem. Instalace této komponenty je nutná na všechny zařízení, které chceme vzdáleně spravovat. Eset Protect Management Agent si

pamatuje nadefinované bezpečnostní scénáře, a to díky tomu, že se nachází fyzicky na klientské stanici. Nasazení probíhá přes Eset Protect Web Console na stanice načtené z Active Directory nebo nalezené přes nástroj RD Senzor. Eset Protect Management může být nasazen na stanice ručně.

- **Rogue Detection Sensor (RD Senzor)** – nástroj pro přidání nových zařízení do konzole. Nachází nespravovaná zařízení v síti a posílá o těchto zařízeních informaci na Eset Protect Server. RD Senzor uchovává v paměti zařízení, které již objevil. Tudíž neodesílá duplicitní informace.
- **Mobile Device Connector** – zajišťuje komunikaci mezi mobilními zařízeními s OS Android a nástrojem Eset Protect. Podporován je i operační systém iOS.
- **ESET PROTECT Virtual Appliance** – nástroj pro provoz ve virtuálním prostředí.
- **Apache HTTP Proxy** – je možno využít jako cache pro distribuci aktualizací detekčních modulů a instalačních balíčků. Další využití je v přesměrování komunikace mezi Eset Protect Management Agentem a Eset Protect Serverem.
- **Mirror tool** – nástroj pro aktualizace modulů v offline sítích.
- **ESET Remote Deployment tool** – nástroj pro vzdálené nasazení Eset Management Agenta s bezpečnostním řešením.
- **ESET Business Account** – licenční portál pro správu licencí.
- **ESET Enterprise Inspector** – nástroj pro sběr dat z koncových zařízení. Nabízí detekci incidentů, správu incidentů včetně reakcí na incidenty, detekci anomálií, detekci porušení firemní politiky.[35] [36]

3.2 HW požadavky a podporované hypervizory

V kapitole budou uvedeny hardwarové požadavky na zařízení, na kterém bude provozován nástroj Eset Protect. SQL server může sdílet stejné prostředky s Eset Protect serverem. Provoz na stejném zařízení zvýší výkon nástroje Eset Protect. Tabulka je dělena podle počtu klientů, které bude Eset Protect spravovat. Firma Eset doporučuje pro 10 000 a více klientů instalaci databáze na samostatný disk z důvodu zvýšení výkonu SQL serveru. V tabulce je uvedena minimální hodnota pro celkový počet I/O operací za sekundu (IOPS). Doporučená hodnota na připojeného klienta je 0,2 IOPS. Výrazně se doporučuje použití SSD disků oproti HDD z důvodů vetší rychlosti SSD. [37]

Tabulka 1. Hardwarové požadavky [37]

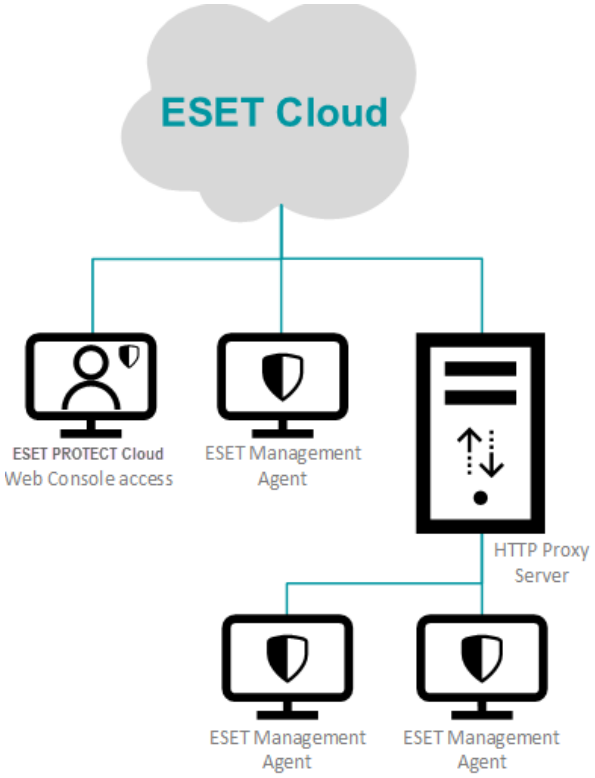
<table>
<tr><td rowspan="2">Počet klientů</td><td colspan="4">Eset Protect Server + SQL databázový server</td></tr>
<tr><td>Počet jader</td><td>RAM (GB)</td><td>Disková jednotka</td><td>IOPS Disku</td></tr>
<tr><td>Do 1 000</td><td>4</td><td>4</td><td rowspan="2">Jeden</td><td>500</td></tr>
<tr><td>5 000</td><td>8</td><td>8</td><td>1 000</td></tr>
<tr><td>10 000</td><td>8</td><td>16</td><td rowspan="3">Samostatné</td><td>2 000</td></tr>
<tr><td>50 000</td><td>16</td><td>32</td><td>10 000</td></tr>
<tr><td>100 000</td><td>16</td><td>32 a vice</td><td>20 000</td></tr>
</table>

Seznam podporovaných hypervizorů:

- Citrix XenServer
- Microsoft Hyper-V
- VMware vSphere
- VMware ESXi
- Vmware Workstation
- Vmware View
- Oracle VirtualBox [38]

3.3 Eset Protect Cloud

Nástroj Eset Protect Cloud je alternativou k on-premise řešení a je určen pro správu bezpečnostních produktů. U cloud řešení není nutné provádět instalaci a počáteční konfiguraci, jelikož je aplikace navržena k okamžitému použití. Hlavním rozdílem oproti on-premise řešení je, že Eset Protect Cloud funguje na cloudovém prostředí, které spravuje společnost Eset. Mezi další rozdíly patří omezení v počtu spravovaných zařízení, u on-premise varianty je limit stanoven od HW prostředků serveru, kde je cloud řešení je omezeno na 25 000 klientů. Dále u Eset Protect Cloud schází služba Eset Enterprise Inspector a není podporována virtualizace pomocí VAgentHost a Eset Virtualization Security. Narozdíl od on-premise řešení nelze přidávat počítače ručně nebo pomocí lokální instalace agenta, jelikož se u cloud verze se o správu certifikátů stará společnost Eset.[39] [40]



Obrázek 10. Schéma Eset Protect Cloud [39]

3.4 Představení konkurence

3.4.1 Avast Business Antivirus Pro Plus

Firma Avast má ve své nabídce kompletní bezpečnostní řešení sítí a koncových zařízení pro malé a střední firmy. Správa je umožněna z jedné integrované platformy díky cloudovému řešení, využívající strojového učení s behaviorální detekcí a detekci založenou na signaturách.

Řešení je podporováno na všech počítačích a serverech, kde ochranu zajišťuje pomocí sandboxování[2] a testování podezřelého obsahu. Detekce malwaru probíhá ještě před jeho spuštěním. Součástí je i VPN, vestavěný firewall a emailový štít. Toto bezpečnostní řešení není podporováno na mobilních zařízeních. [41]

3.4.2 Norton Small Business

Bezpečnostní řešení s podporou 20 koncových zařízení, kde je kompatibilita zaručena se všemi zařízeními s Windows, iOS a Android. Řešení disponuje jednoduchým nasazením díky rychlému nastavení a správě přes cloud. Organizace škodlivých souborů probíhá podle jejich reputace a chování. Tímto způsobem je možné soubory při dalším výskytu rychleji zablokovat. Bezpečnostní řešení disponuje ochrannou proti malware, ransomware a zero day exploitům[3]. Dalšími funkcemi jsou upozornění na potencionálně nebezpečný stažený soubor a na nebezpečné odkazy. [41]

3.4.3 McAfee Total Protection

Dalším bezpečnostním řešením může být software od společnosti McAfee, nabízející ochranu založenou na strojovém učení v reálném čase a zabezpečení webu. Bezpečnostní software funguje na pozadí, ke kontrolám zařízení dochází při nečinnosti zařízení a díky tomu je pro uživatele skoro nezjistitelný. Systémové požadavky pro bezpečnostní software nejsou velké a díky tomu nezatěžuje pracovní stanice. Software disponuje ochranou proti malwaru, integrovanou bránou firewall, správou hesel a anti – phishing technologii pro

[2] Sandboxování se využívá k testování potencionální hrozby v bezpečném virtuálním prostředí.[42]
[3] Zero day eploit je útok za využití bezpečnostní chyby v softwaru, na kterou zatím neexistuje aktualizace v podobě bezpečnostní záplaty.[43]

ochranu emailových schránek. Systém umí rozpoznat typické chování pro malware, které blokuje. Bezpečnostní řešení může být nasazeno v podniku do 10 zařízení. [41]

3.4.4 Porovnání

Pro bakalářkou práci jsem vybral bezpečnostní balíček od společnosti Eset a konkrétně se jedná o nástroj Eset Protect. Byl vybrán z důvodu preference on – premise řešení, která u konkurenčních služeb chybí. V dalších prvcích jsou již nabízené služby srovnatelné všichni výrobci nabízí standardní ochranu proti malware, anti – phishing ochranu a vestavěný firewal, vyjma řešení od společnosti Norton. Mínusem vybraného řešení Eset Protect je absence VPN. Počet klientských stanic je v rozmezí pro male až střední firmy dostačující u všech výrobců.

Tabulka 2. Srovnání s konkurencí[37][41]

	Eset Protect	Avast Business Antivirus Pro Plus	Norton Small Business	McAfee Total Protection
On – premise	Ano	Ne	Ne	Ne
Cloud based	Ano	Ano	Ano	Ano
VPN	Ne	Ano	Ne	Ano
Firewall	Ano	Ano	Ne	Ano
Ochrana před phishingem	Ano	Ano	Ano	Ano
Podpora android a iOS zařízení	Ano	Ne	Ano	Ano
Počet klientských stanic	Až 100 000	1-100	1–20	1-10
Konzole pro správu	Ano	Ano	Ano	Ano

3.5 Závěrečné shrnutí

Poslední kapitola teoretické části je věnována vybranému bezpečnostnímu řešení. Jsou zde popsány jeho části, ze kterých se bezpečnostní balíček skládá a analyzovány hardwarové požadavky dle počtu koncových klientů. Je zde zmíněno i cloudové řešení, které může být nasazeno místo varianty on – premise. Řešení on-promise je použito dále v praktické části. V závěru kapitoly jsou popsány a porovnány konkurenční bezpečnostní řešení. Vybraný bezpečnostní balíček od firmy Eset se vyznačuje malou zátěží systému oproti konkurenci. Dále disponuje ochranou proti phishingu nebo například zabudovaným firewallem. Velkou výhodou je možnost řešení on – premise i nasazení v cloudu dle preference.

II. PRAKTICKÁ ČÁST

4 NASAZENÍ BEZPEČNOSTNÍHO NÁSTROJE ESET PROTECT VE FIREMNÍM DOMENOVÉM PROSTŘEDÍ

Praktická část je zaměřena na nasazení vybraného balíčku od společnosti Eset. Úvod praktické části je věnován popisu testovacího prostředí. Následně je uveden samotný postup při nasazení bezpečnostního balíčku. Je zde popsána instalace ve virtuálním prostředí a konfigurace nainstalovaného bezpečnostního řešení. Tu tvoří konfigurace Eset Virtual Appliance, nasazení agentů pro komunikaci serveru a koncových stanic, instalace Endpoint řešení na koncové stanice a další. V poslední části jsou analyzovány nejběžnější události, které můžeme pomocí nástroje Eset Protect řešit.

Postup praktické části:

- Popis tvorby testovacího prostředí
- Instalace Eset Virtual Appliance v Hyper – V
- Konfigurace nástroje Eset Protect
- Řešení nejčastějších problémů v rámci Eset Protect

5 TESTOVACÍ PROSTŘEDÍ

Pro potřeby této bakalářské práce bylo vytvořeno testovací prostředí, které mělo simulovat typické firemní prostředí a následně zde byly testovány jednotlivé funkcionality produktu Eset. Testováno bylo na notebooku (Intel i7-1165G7, 32GB RAM a 1TB SSD) s Windows 10 Pro.

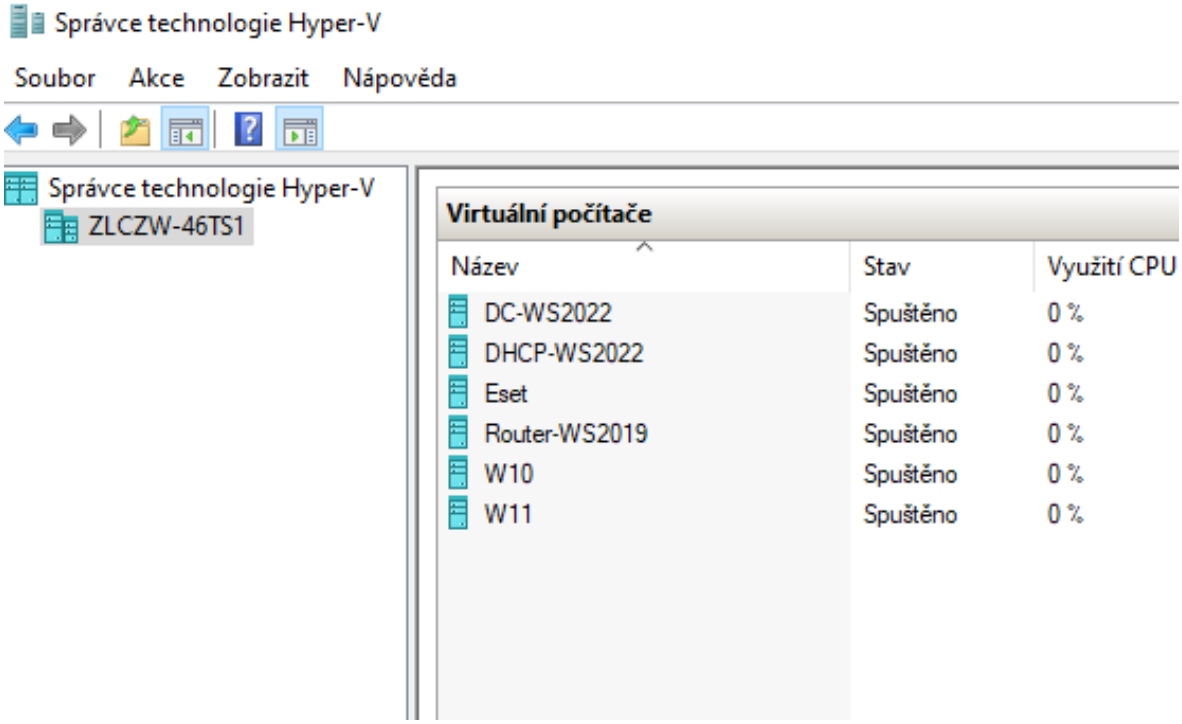
Jako hypervisor jsem zvolil Microsoft Hyper-V vzhledem k nativní podpoře ve Windows 10 Pro. Zde bylo vytvořeno několik serverů a dvě koncové stanice s rozdílnými operačními systémy.

Role serverů, které bylo potřeba vytvořit: doménový řadič (DC), DNS, DHCP a router (vytvoření internetové konektivity pro jednotlivé virtuální stroje). Servery byly postaveny v rámci testování na Windows Server 2022 Std a Windows Server 2019 Std.

Klientské stanice byly vytvořeny s operačními systémy Windows 10 a Windows 11.

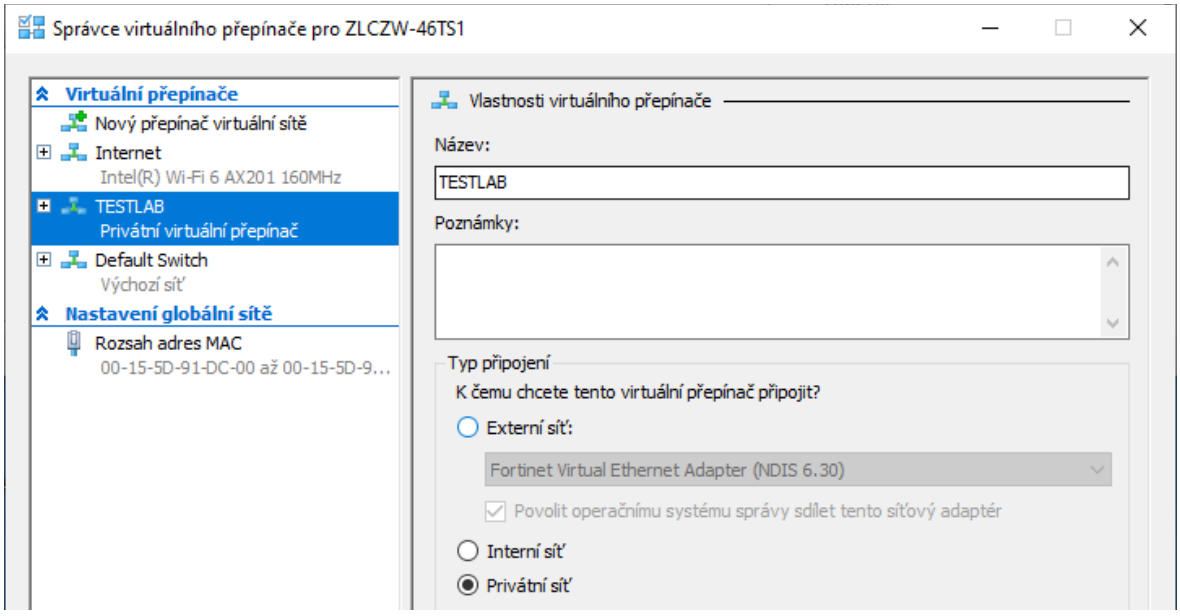
Soupis virtuálních strojů v rámci testovacího prostředí:

- DC-WS2022 – DC, DNS server (Windows Server 2022),
- DHCP-WS2022 – DHCP server (Windows Server 2022),
- Eset – Eset Protect Virtual Appliance (CentOS),
- Router-WS2019 – routování v rámci testovací LAN (Windows Server 2019),
- W10 – koncová klientská testovací stanice (Windows 10 Pro),
- W11 – koncová klientská testovací stanice (Windows 11 Pro).



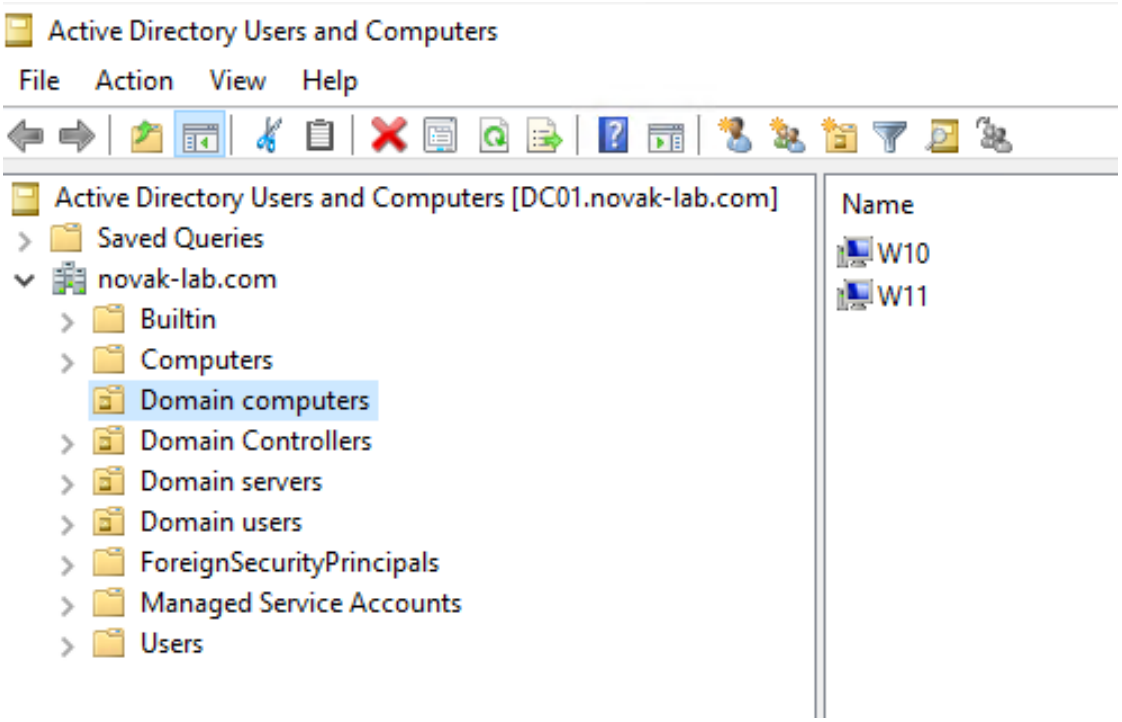
Obrázek 11. Rozhraní Hyper – V managera s přehledem testovacích strojů

Kvůli propojení jednotlivých virtuálních strojů bylo zapotřebí nakonfigurovat dva virtuální přepínače. Jeden pro interní komunikaci mezi nimi (název TESTLAB) a druhý pro přístup k internetu (název Internet), který je připojen pouze k virtuálnímu serveru Router-WS2019.



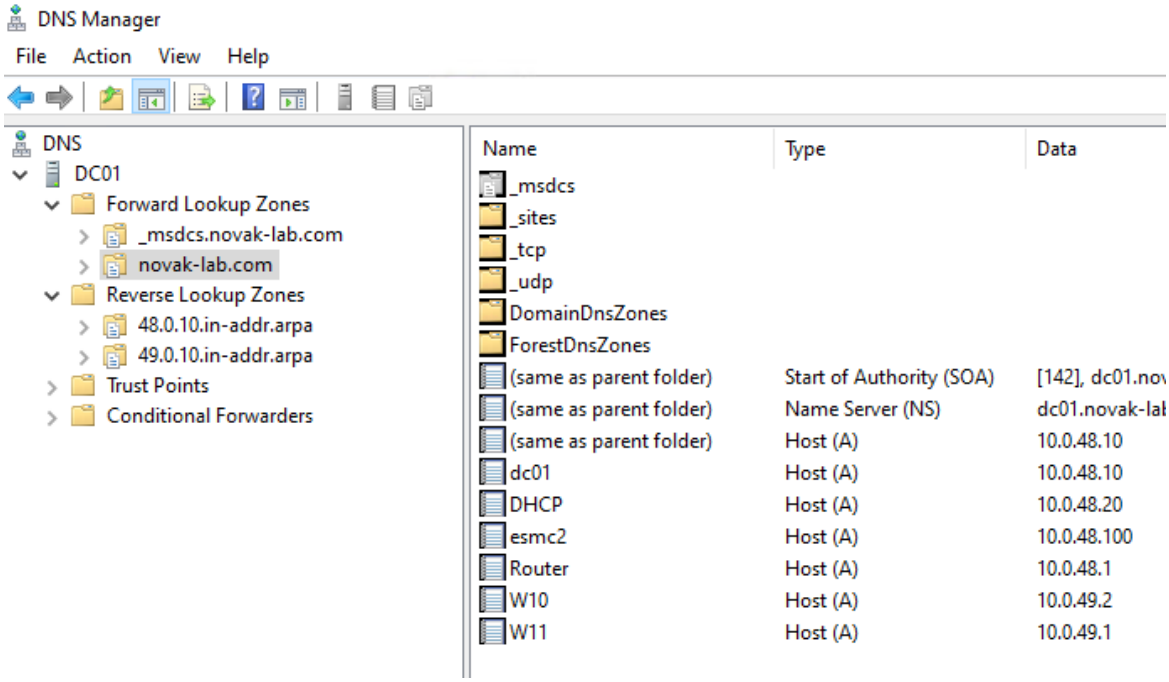
Obrázek 12. Hyper – V správce virtuálního přepínače

Na doménovém kontroleru byla vytvořena testovací doména **novak-lab.com** a vytvořena základní struktura organizačních jednotek v rámci Active Directory.



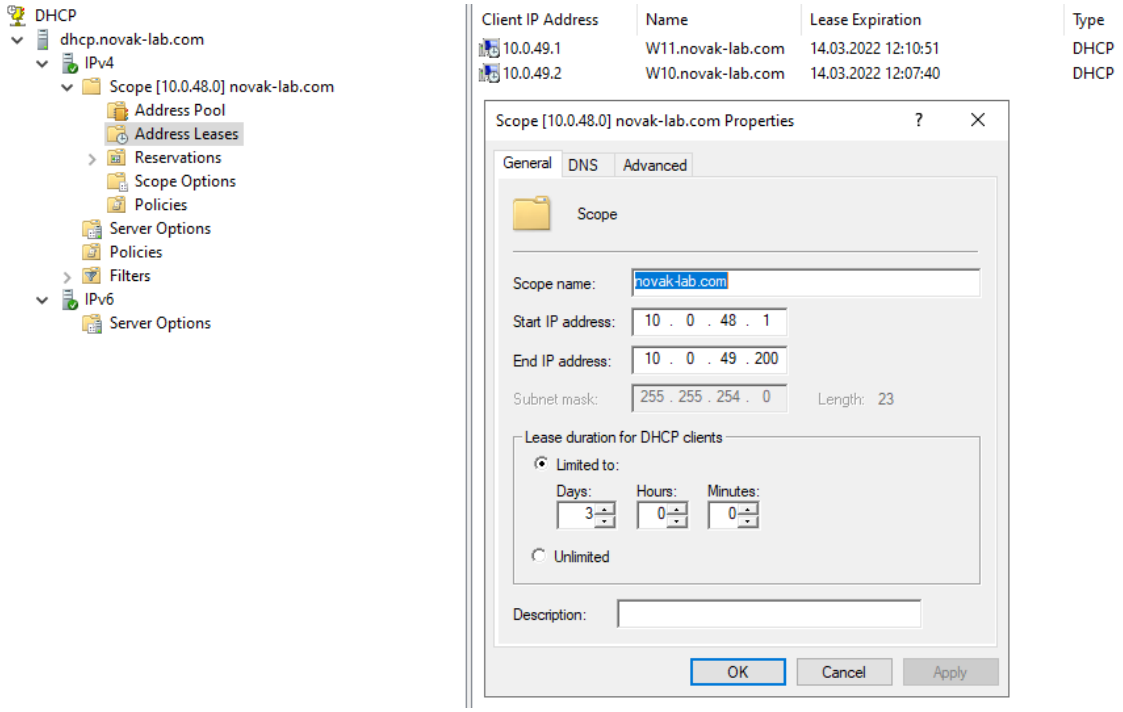
Obrázek 13. Testovací klienti v konzoli Active Directory Users and Computers

Posléze bylo potřeba na DNS serveru nastavit jednotlivé záznamy pro servery a koncové stanice, zejména pro Eset Appliance, a to včetně nastavení reverzní zóny pro jednotlivé rozsahy.



Obrázek 14. Nastavení statických DNS záznamů

Na DHCP serveru byl nakonfigurován rozsah 10.0.48.1–10.0.49.200 s tím, že byl vyloučen rozsah 10.0.48.1/24 z DHCP a je určen pro servery.

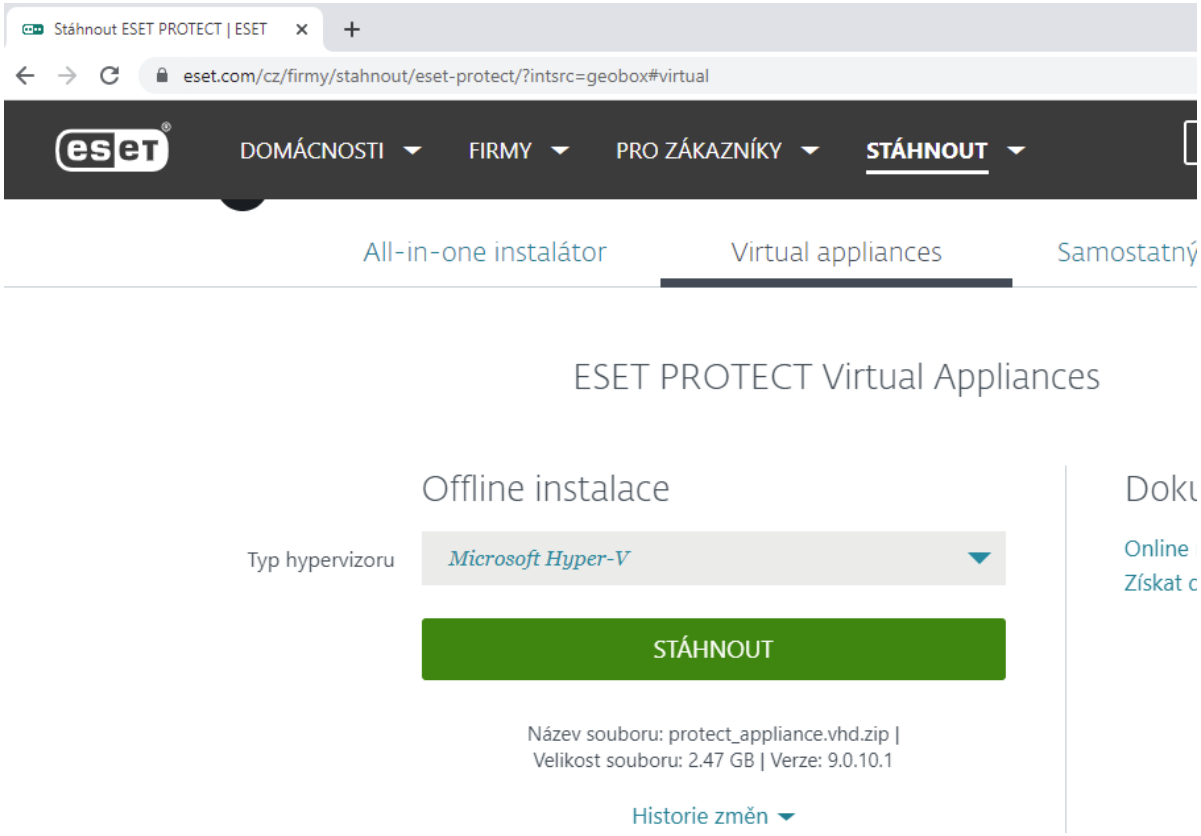


Obrázek 15. Konfigurace DHCP rozsahu IP adres

6 INSTALACE ESET VIRTUAL APPLIANCE NA HYPER-V

Pro provedení instalace v prostředí Microsoft Hyper-V je nejprve potřeba stáhnout předpřipravený virtuální disk s Eset Virtual Appliance a následně tento využít pro nový virtuální počítač.

Prvním krokem je stažení předpřipraveného virtuálního VHD disku pro Microsoft Hyper-V ze stránek Esetu a tento posléze extrahovat pomocí nástroje jako Tar nebo 7-zip k dalšímu použití.

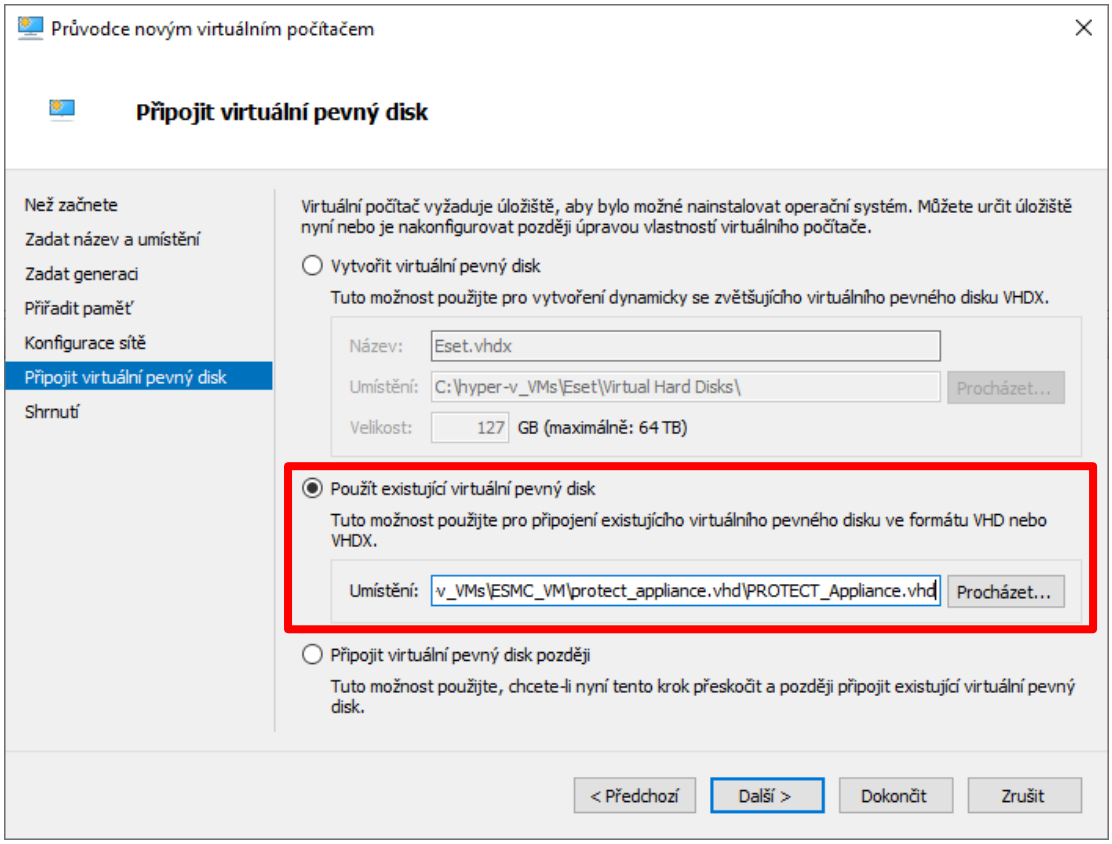


Obrázek 16. Webová stránka pro stažení virtuálního disku formátu VHD [44]

Následným krokem je spuštění Hyper-V Managera a vytvoření nového virtuálního počítače, na kterém budeme provozovat Eset Protect Virtual Appliance. Při vytváření je nutné zvolit, že se jedná o 1. generaci virtuálního počítače, kvůli podpoře vhd virtuálního disku, který byl stažen ze stránek Esetu. V generaci 2 jsou podporovány pouze vhdx disky.

Virtuálnímu počítači přiřadíme potřebné množství operační paměti a nakonfigurujeme jej do naší testovací LAN, kde by již měl získat svou IP adresu pro prvotní nastavení z DHCP serveru.

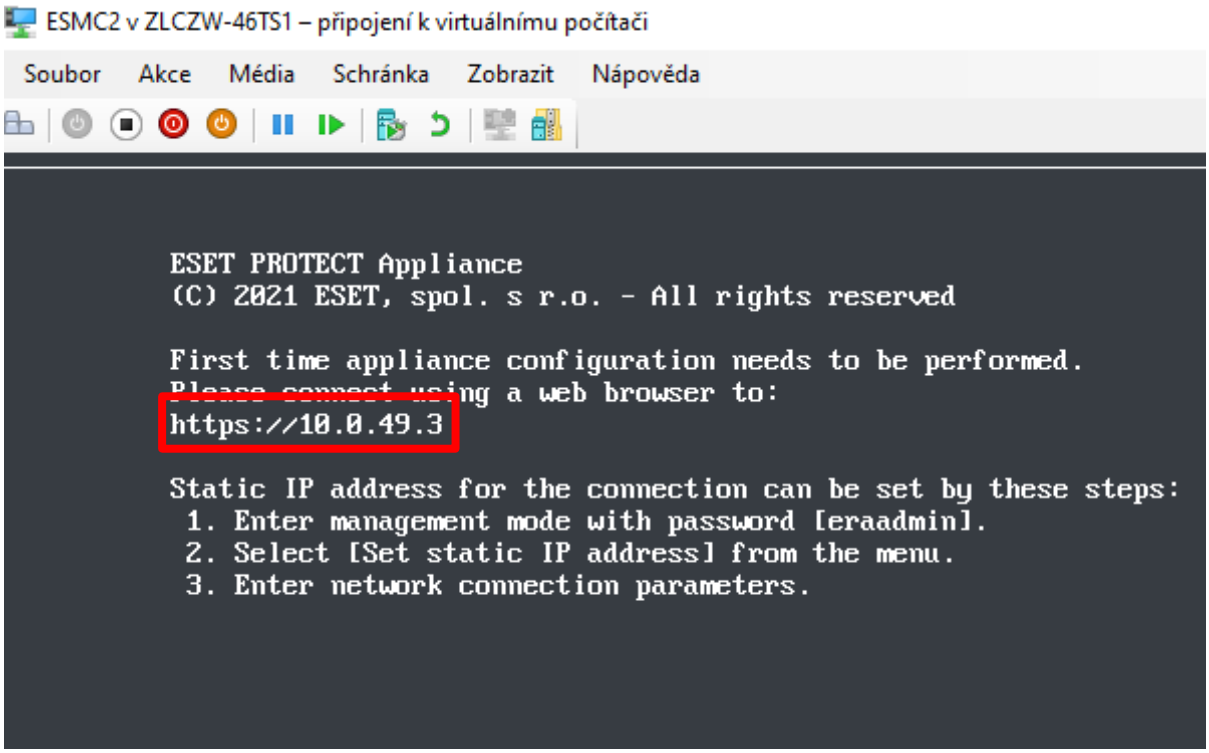
V dalším kroku provedeme připojení staženého virtuálního VHD disku k nově vytvořenemu virtuálnímu počítači. Zvolíme možnost použití existujiciho virtuálního disku a vybereme umístení kde se nachazí stažený virtuální pevný disk (Obrázek 17).



Obrázek 17. Připojení staženého virtuálního disku k virtuálnímu počítači

Po vytvoření virtuálního počítače je možno jej zapnout a počkat, jestli vše proběhne v pořádku. Pokud ano, tak by již měl následně naběhnout do úvodní obrazovky, jak je možné zkontrolovat přes náhled na virtuální počítač.

IP adresu si server korektně převzal z DHCP serveru, tudíž lze rovnou začít s konfigurací Eset Protect Virtual Appliance přes jeho webové rozhraní, které je v našem případě na URL: https://10.0.49.3 (Obrázek 18).



Obrázek 18. Obrazovka Eset Protect Appliance s jeho management IP adresou

7 ESET KONFIGURACE

Po úspěšné instalaci Eset Appliance v Hyper-V můžeme přejít k samotné konfiguraci nástroje Eset Protect. Prvním krokem je konfigurace nainstalované Eset Appliance, které provedeme přes webové rozhraní a je popsáno v bodu níže.

Dalším krokem je přiřazení 30denní zkušební licence, jenž zpřístupní jednotlivé produkty, které můžeme využívat.

Po přiřazení zkušební licence následuje instalace Eset Agenta. Tento krok je velmi důležitý, protože Eset Agent zajišťuje komunikaci mezi koncovými produkty a Eset Protect serverem. V práci je popsána varianta nasazení přes skupinové politiky (Group Policy). Nasazení můžeme provést i jinými způsoby, přičemž dané možnosti nalezneme na webových stránkách společnosti Eset.

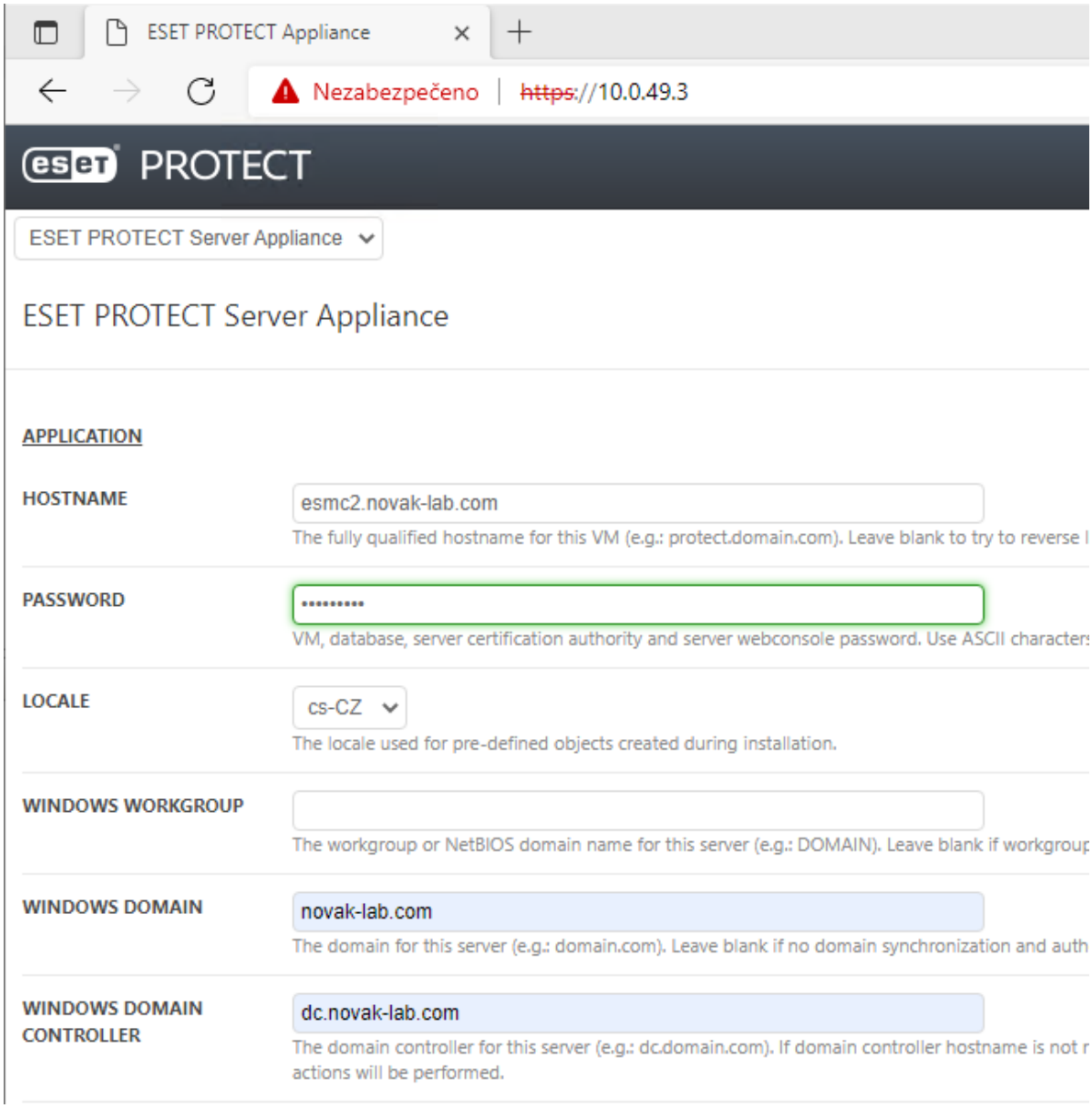
Následně je zde popsáno nasazení antiviru, který se stará o zajištění bezpečnosti na klientských stanicích.

7.1 Základní nastavení Eset Protect Appliance

Pro prvotní nastavení je potřeba se přihlásit přes webové rozhraní. Adresu pro správu známe již z předchozího bodu.

Nastavíme plný doménový název (hostname) pro appliance. V našem případě jsem zvolil hostname esmc2.novak-lab.com. Zadáme heslo pro administrátorský účet (název výchozího účtu je Administrator).

Dále je zapotřebí nastavit správnou doménu: novak-lab.com a doménový řadič: dc.novak-lab.com. Aby se server automaticky přidělil do domény, je nutné vyplnit i potřebné přihlašovací údaje pro jeho ověření v doméně.



Obrázek 19. Prvotní nastavení Eset Appliance

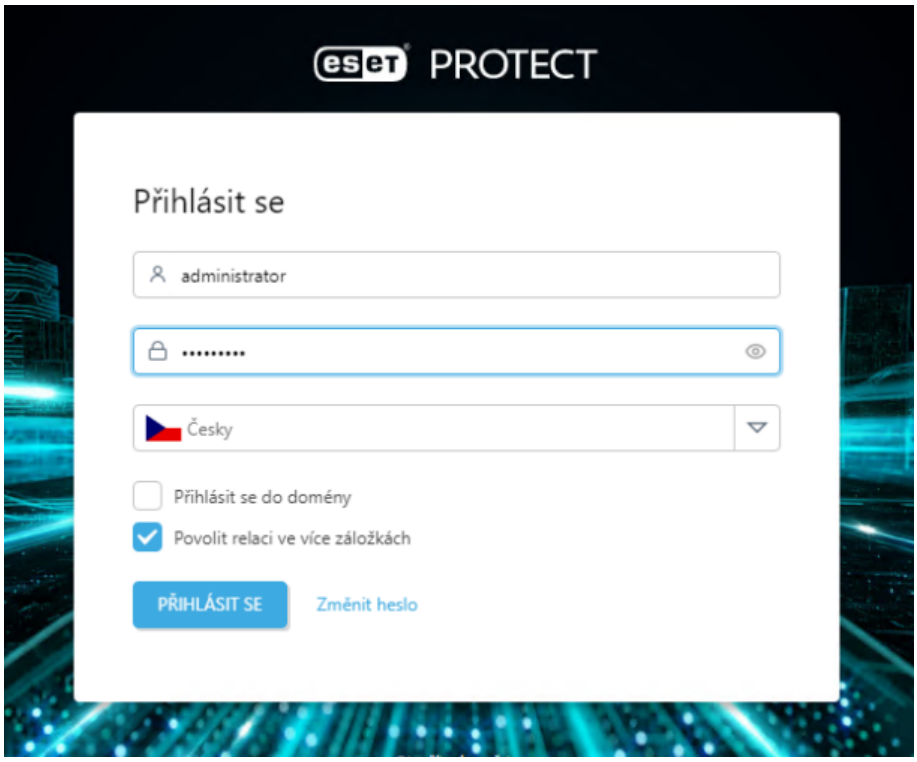
Následně již vyplníme síťové nastavení pro daný server a potvrdíme. Dojde k instalaci a nastavení všeho potřebného automaticky.

Po úspěšné konfiguraci Eset Protect Appliance je možné se přihlásit do administrativního rozhraní Eset Protect a přiřadit zkušební licenci. Přihlášení již proběhne přes nově zvolenou IP adresu pro správu a heslo administrátora.

7.2 První přihlášení do Eset Protect a přirazení zkušební licence

Přihlásíme se zvolenými údaji, které jsem zadal při konfiguraci serveru v předchozím bodě.

Rozhraní je dostupné přes https již na nové IP adrese. Případně lze využít již i hostname.



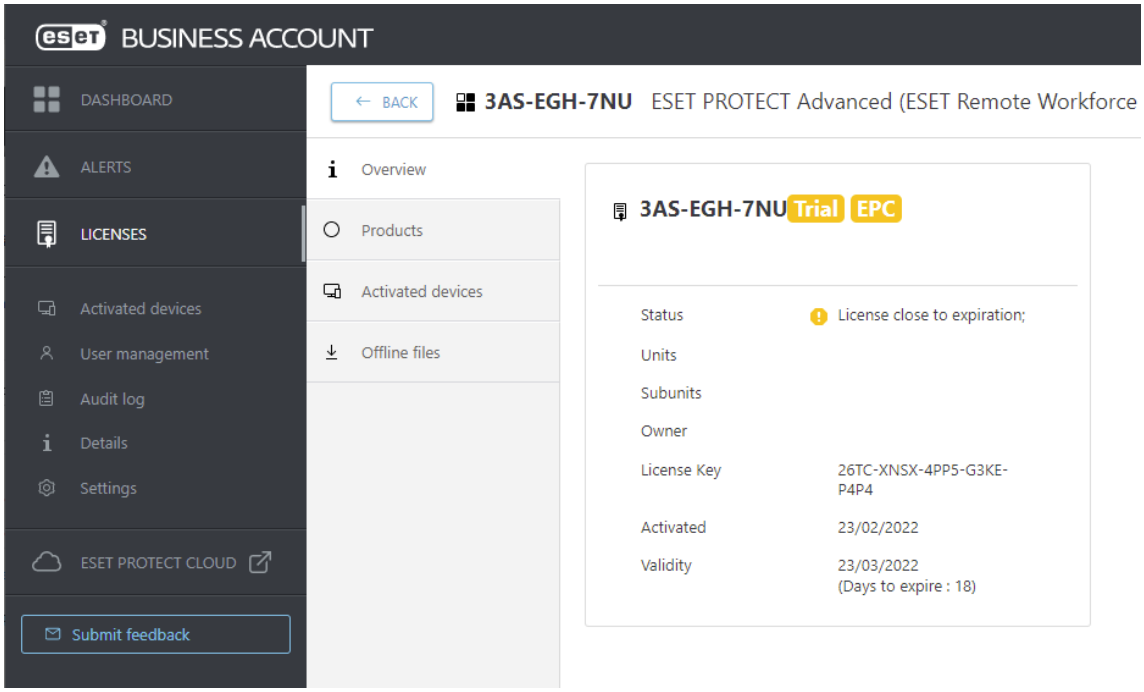
Obrázek 20. Obrazovka přihlášení k administraci Eset Protect

Následně server zalicencujeme zkušební licencí, kterou jsem přiřadil k vytvořenému účtu na portále Eset. Tato licence je platná 30 dní a umožňuje nasadit Eset až na 50 zařízení. Pomocí přihlášení tímto účtem dojde ke spojení s danou zkušební licencí.

Při přidělování licence můžeme vybírat mezi způsoby, jakým chceme licenci přidělit. Volba se provádí z tří možností:

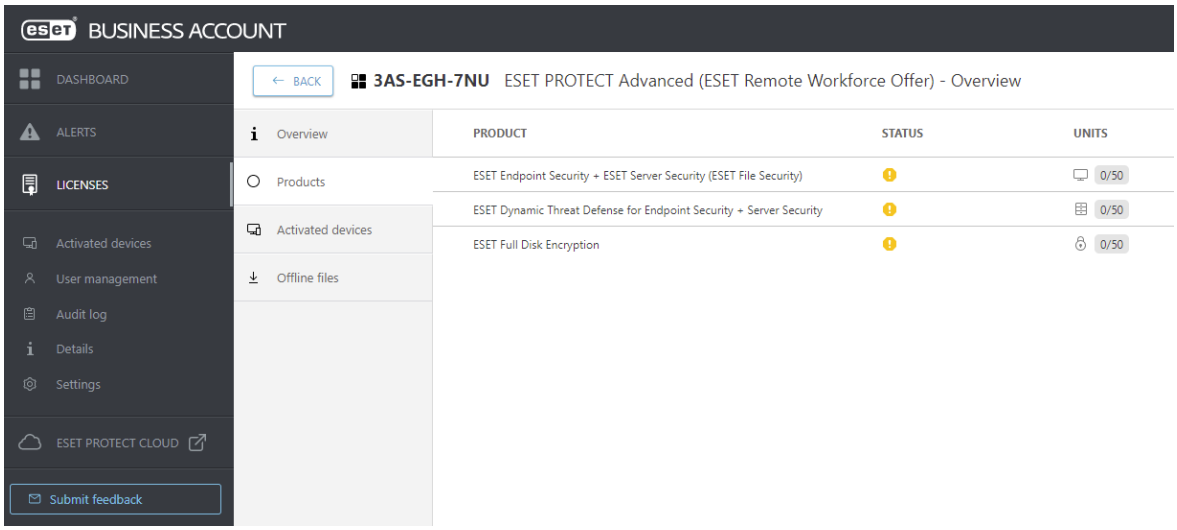
- ESET Bussines Account nebo ESET MSP Administrator
- Licenční klíč
- Offline licenční soubor

Byl zvolen první způsob zalicencování produktu a zadány přihlašovací údaje. Zkušební licence je určena právě pro tento typ a nelze ji vyplnit napřímo do pole Licenční klíč. Po potvrzení uživatelského jména a hesla dojde k zobrazení přehledu dané licence. Tzn. zobrazení jejího názvu (id licence), statusu, majitele, licenčního klíče a platnosti.



Obrázek 21. Výpis informací o přiřazované licenci

Naše zkušební licence obsahuje tři produkty: Eset Endpoint Security, Eset Dynamic Threat Defense a Eset Full Disk Encryption. V našem případě budeme využívat právě prvního ze zmíněných produktů, a to Eset Endpoint Security.



Obrázek 22. Výpis obsažených produktů v rámci licence

Po potvrzení vyskakovacího okna, zda je vše v pořádku, by již mělo dojít k úspěšnému přidání licencí do Eset Protect. Následně zkontrolujeme v záložce Správa licence.

7.3 Nasazení Eset Agenta pomocí skupinových politik

V rámci organizace v doménovém prostředí Active Directory máme dvě možnosti nasazení Eset Agenta, a to v situaci, kdy budeme chtít tento proces automatizovat. Tzn. agenta nasadit automaticky na každé PC v rámci domény a organizační jednotky „Domain Computers“.

První možností je využití politik v rámci Group Policy a druhou je použití nástroje Microsoft System Center Configuration Manager (nově v rámci nástroje Microsoft Endpoint).

V našem případě budeme popisovat nasazení Eset Agenta právě přes Group Policy.

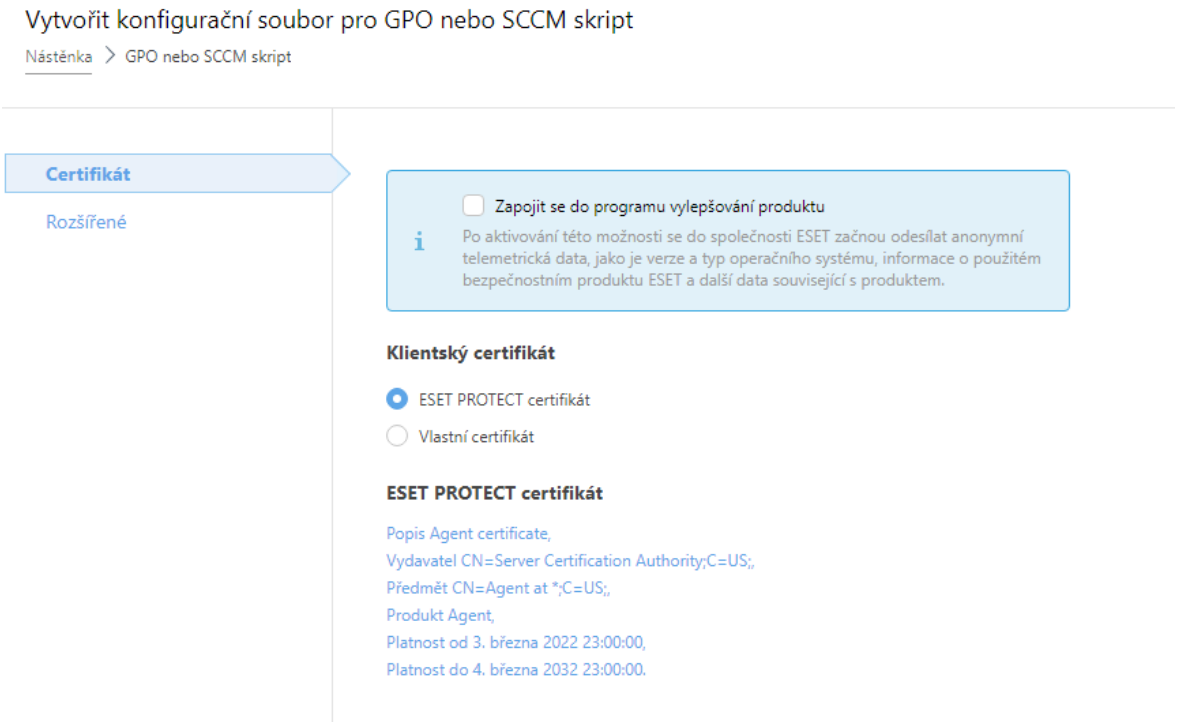
7.3.1 Vytvoření konfiguračního skriptu v rámci Eset Protect

Vytvoříme konfigurační soubor install_config.ini., který obsahuje parametry pro Eset Agenta ke komunikaci s Eset Protect serverem. Konfigurační soubor byl vytvořen pomocí návodu dostupného ze stránek společnosti Eset. [45]

V prvním kroku otevřeme Eset Protect webovou konzoli.

Klikneme Instalační balíčky – Vytvořit instalační balíček – GPO nebo SCCM skript.

Následně následujeme průvodce a vytvoříme skript.

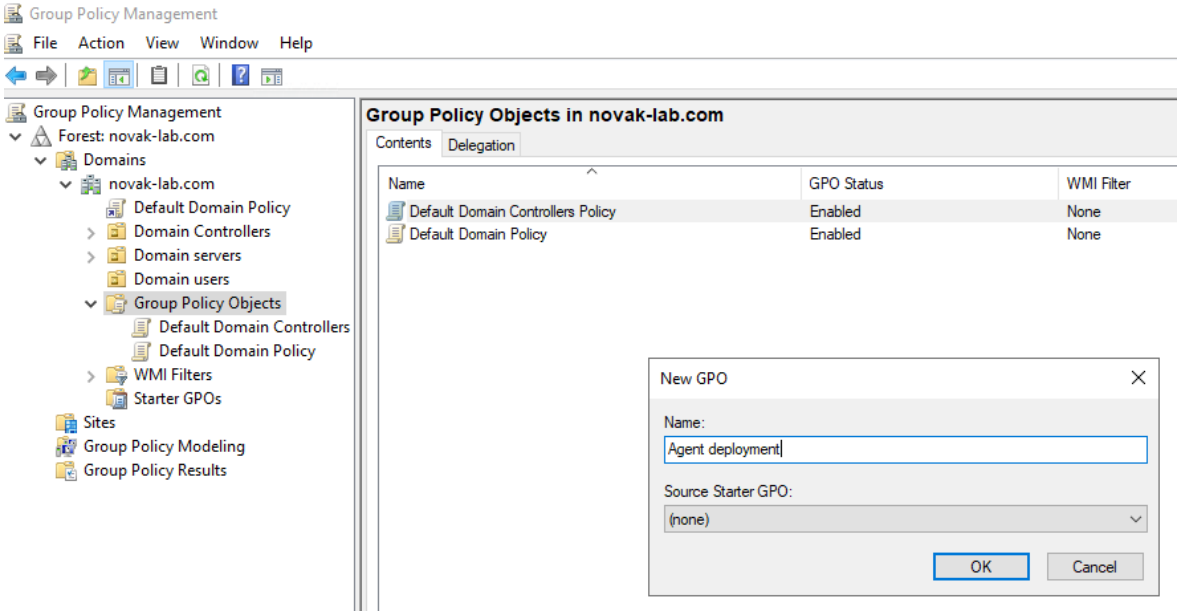


Obrázek 23. Vytvoření konfiguračního souboru pro GPO

Vytvořený soubor install_config.ini následně uložíme do sdílené síťové cesty \\DC01\share.

7.3.2 Nastavení v Group Policy Managementu na doménovém řadiči

Vytvoříme nový objekt v rámci Group Policy Objects s názvem Agent deployment a následně zvolíme jeho editaci.



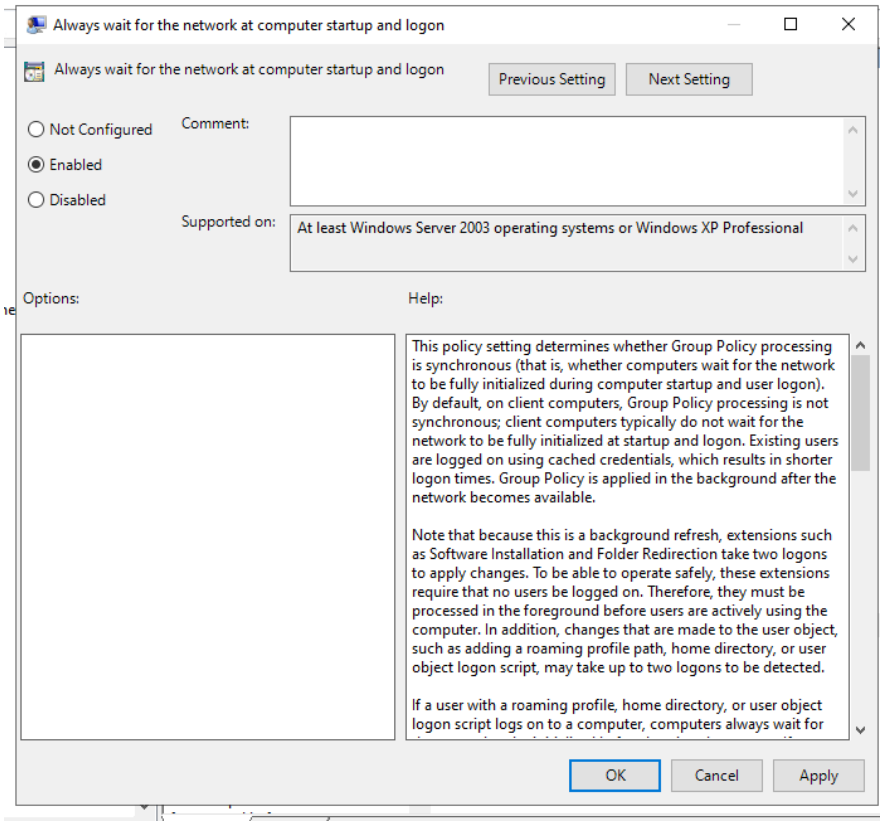
Obrázek 24. Vytvoření nové GPO

Následně v rámci doporučených nastavení od firmy Eset povolíme následující dvě politiky. První politikou je „Always wait for the network at computer startup and logon“. Politiku nastavujeme z důvodu, že klientské počítače obvykle nečekají na úplnou inicializaci sítě při spuštění a přihlášení uživatele. Pokud toto nastavení zásad povolíme, počítače před přihlášením uživatelů počkají na úplnou inicializaci sítě.

Druhá politika se nazývá „Specify startup policy processing wait time“. Pokud toto nastavení zásad povolíme, zásady skupiny použijí tuto administrativně nakonfigurovanou maximální čekací dobu a mají přednost před jakoukoli výchozí nebo systémem vypočtenou čekací dobou. Politika je nastavena z důvodu zajištění potřebného času pro plnou dostupnost sítě před aplikováním politiky na počítač.

Konfiguraci jednotlivých politik provedeme editací politiky s názvem Agent deployment. Přesný postup je následující.

V sekci Computer Configuration – Policies – Administrative Templates: Policy definitions – System – Logon nalezneme položku „Always wait for network at computer startup and logon“, kterou přepneme do stavu Enabled.



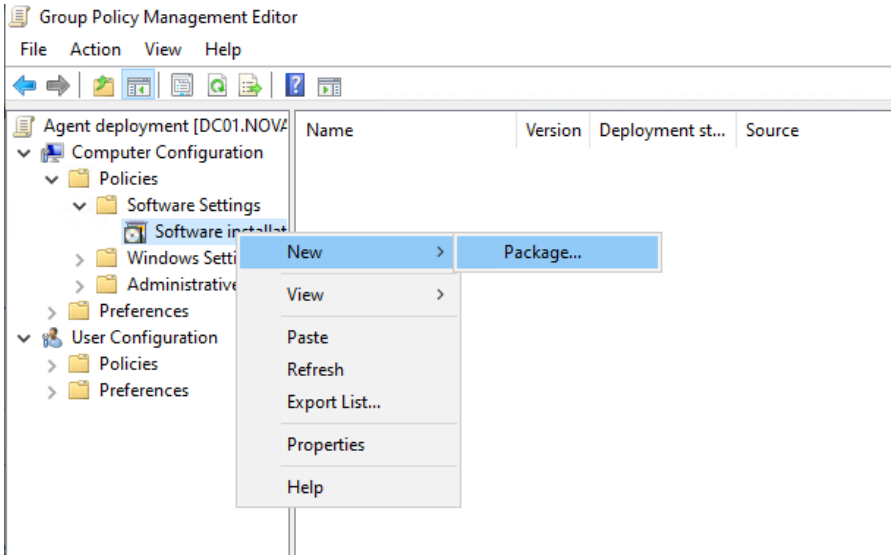
Obrázek 25. Povolení první politiky v rámci GPO

Dále v umístění Computer Configuration – Policies – Administrative Templates: Policy definitions – System – Group Policy vybereme položku „Specify startup policy processing wait time“, zvolíme Enabled a nastavíme 120 sekund.

Následně je potřeba ze stránek Esetu stáhnout samotného agenta (instalační msi balíček s názvem agent_x64.msi), kterého uložíme do dříve vytvořené sdílené cesty \\DC01\Share. Bude se tedy nacházet ve stejné složce jako konfigurační soubor install_config.ini.

V dalším kroku přiřadíme staženého klienta k danému GPO s názvem Agent deployment.

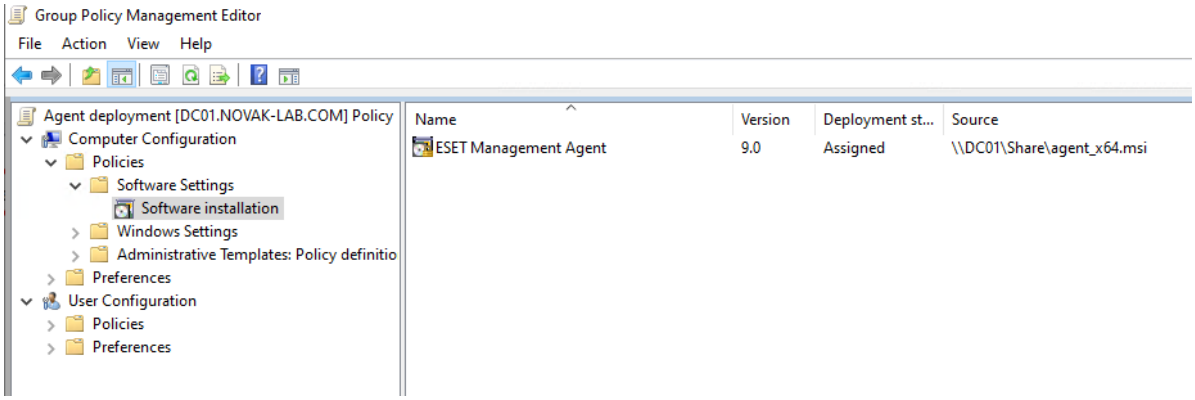
V sekci Computer Configuration – Policies – Software Settings klikneme pravým tlačítkem na Software installation a zvolíme New – Package.



Obrázek 26. Vytvoření nového softwarového balíčku v politice agent deployment

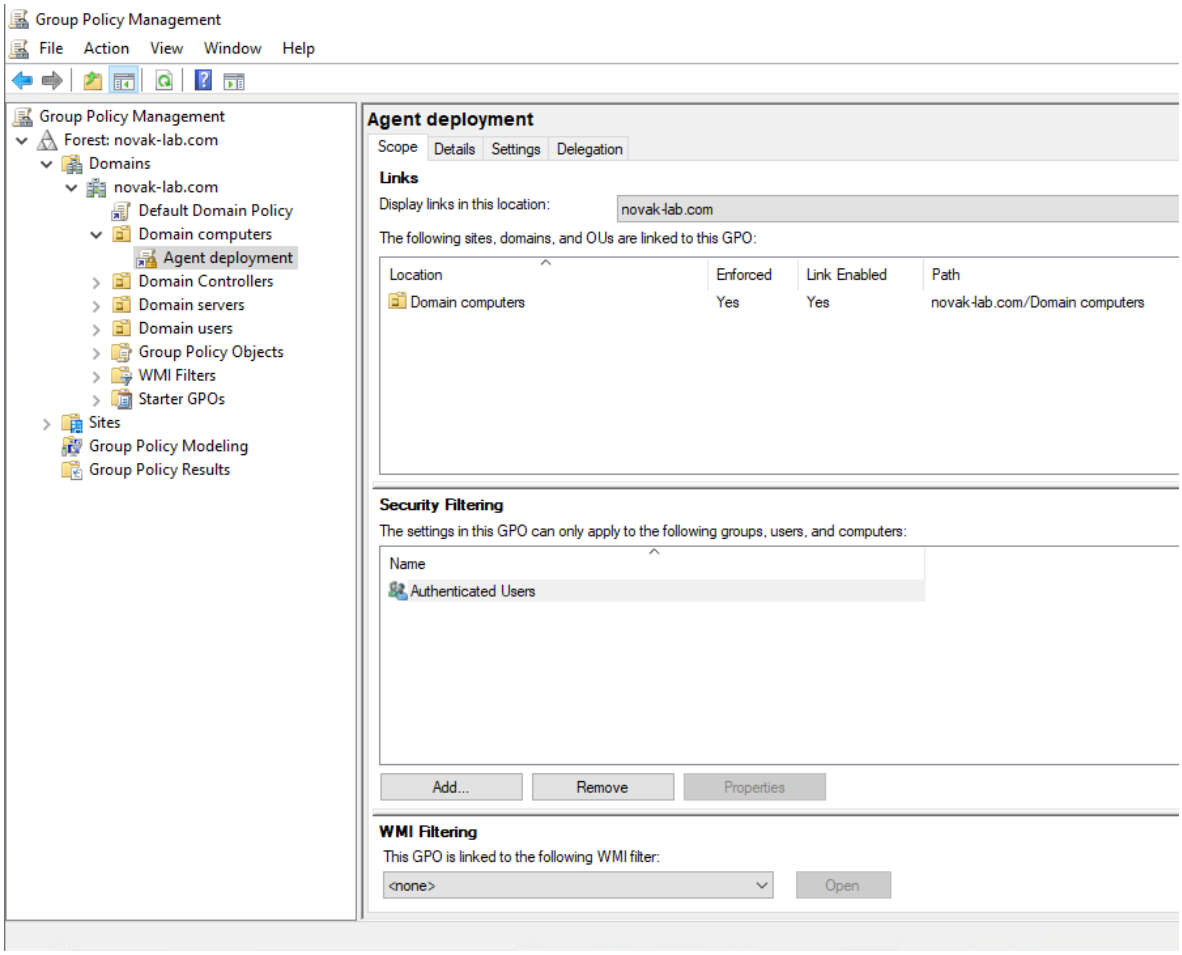
Následně vybereme stažený soubor agent_x64.msi a zvolíme možnost Assigned.

Po tomto kroku máme přidělen instalační soubor Eset Agenta k danému GPO, jak můžeme vidět na obrázku níže.



Obrázek 27. Přidání instalačního balíčku

Následně danou politiku přiřadíme k organizační jednotce Domain Computers, ve které jsou umístěny testovací koncové stanice.

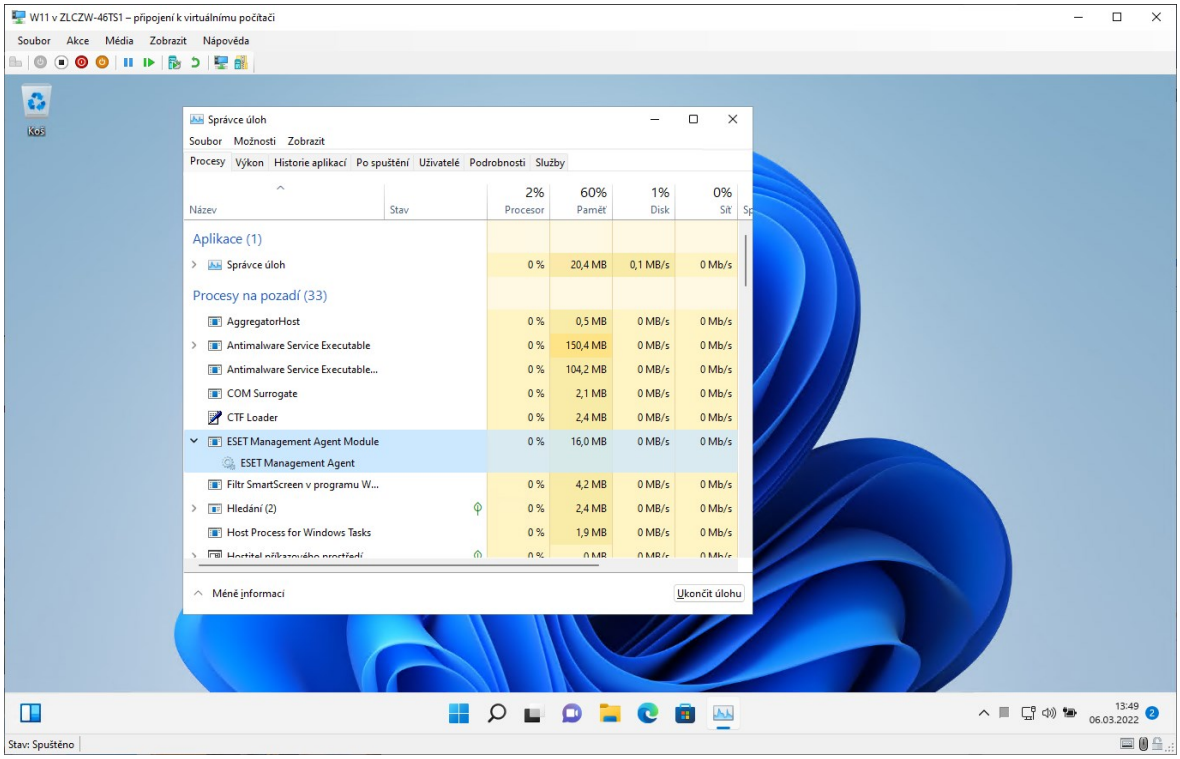


Obrázek 28. Přiřazení politiky pro všechny doménové počítače

7.3.3 Kontrola instalace Eset Agenta

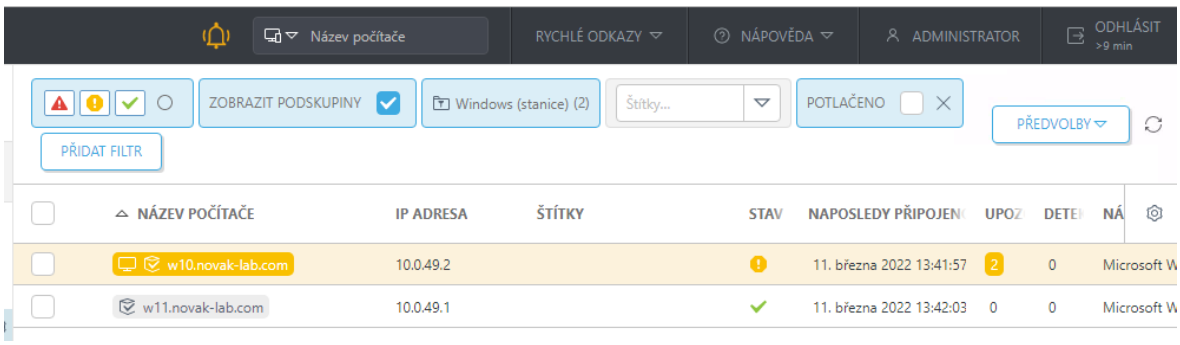
Na testovacích klientských stanicích (Windows 10 i 11) jsem spustil příkaz gpupdate pro aktualizaci skupinových politik a následně stanici restartoval.

Na obou se po naběhnutí operačního systému a několika minutách nainstaloval Eset Agent. K ověření instalace byl použit správce úloh, kde je vidět v seznamu procesů Eset Management Agent, viz obrázek níže.



Obrázek 29. Kontrola provedení instalace Eset Agenta na koncové stanici W11

Stejně tak se obě testovací stanice objevily v rozhraní Eset Protect, kde jsou automaticky zařazeny ve skupině Windows (stanice) a je možné je začít vzdáleně spravovat.



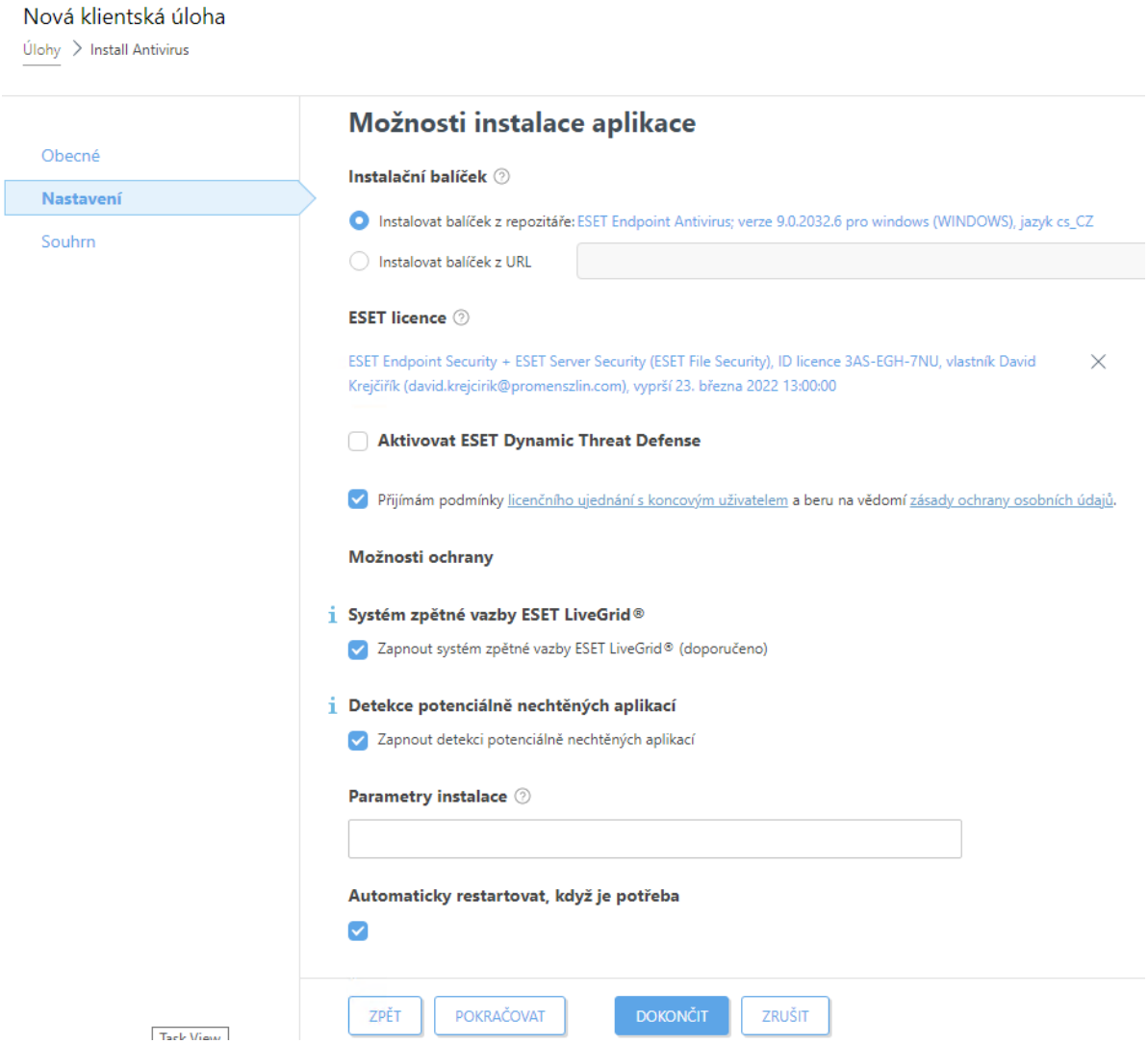
Obrázek 30. Kontrola přiřazení koncových stanic do Eset Protect

7.4 Instalace programu Eset Endpoint Antivirus

7.4.1 Nastavení úlohy pro instalaci v rámci Eset Protect

K nasazení antivirového programu Eset je potřeba vytvořit samostatnou úlohu. Po jejím spuštění se následně automaticky nainstaluje Eset Antivirus na všechny klientské stanice, kterou jsou přiděleny do skupiny Windows (stanice) v rámci Eset Protect.

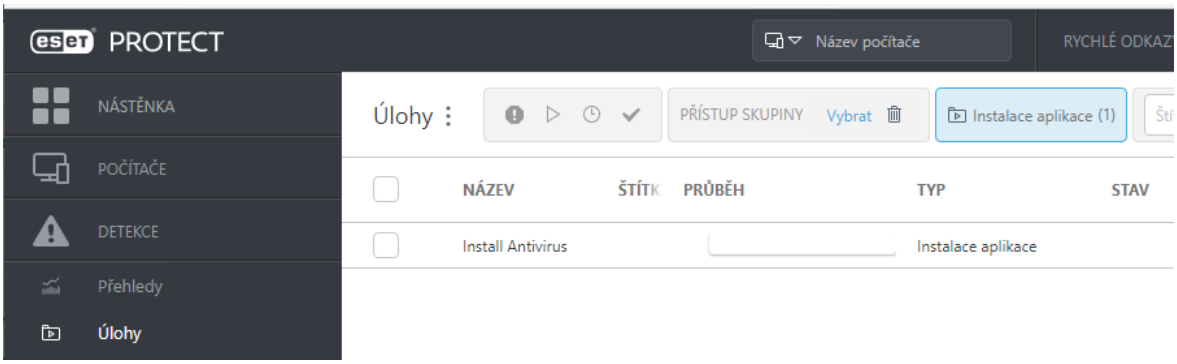
Zvolíme sekci Úlohy a pomocí možnosti nová klientská úloha ji vytvoříme. Na začátku tvorby nové klientské úlohy zvolíme její název a popis dané úlohy. Dále přejdeme k nastavení klientské úlohy. Zde z repozitáře vybereme požadovaný produkt k instalaci, v našem případě Eset Endpoint Antivirus verze 9 v českém jazyce a zvolíme dokončit.



Obrázek 31. Nová klientská úloha a její nastavení

Po vytvoření úlohy je potřeba nastavit podmínku spuštění. Zde je nutné stanovit její popis a následně určit cíle, na které se má úloha aplikovat. V našem případě na klientské stanice se systémem Windows. Podmínka spuštění je nutná k přesnému nastavení doby aplikování klientské úlohy, v rámci testování jsem vždy volil aplikovat ihned. Tzn. ihned po dokončení se úloha začne aplikovat na jednotlivé stanice dle podmínky. Je ale možné nastavit libovolný čas spuštění a dobu expirace dané úlohy.

Dále danou úlohu můžeme zkontrolovat, případně upravit pod nabídkou Úlohy.

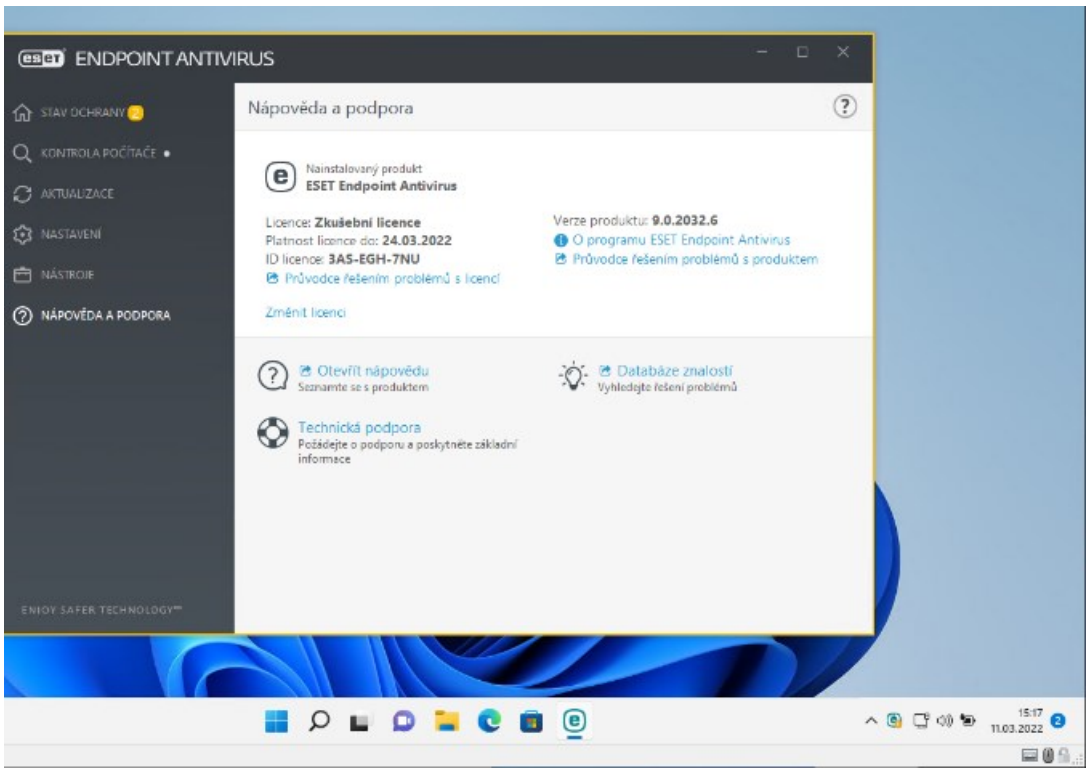


Obrázek 32. Zobrazení vytvořené úlohy v nastrojí Eset

Klientská úloha byla využita k instalaci Eset Endpoint antiviru na všechny klientské stanice. Při instalaci softwaru na větší počet klientských stanic vytvořením klientské úlohy ušetříme čas. Nastavením skupiny, na kterou je klientská úloha aplikována, zaručíme bezobslužnou instalaci softwaru pouze na vybrané koncové stanice.

7.4.2 Kontrola instalace antiviru na koncových stanicích

Po spuštění úlohy došlo k automatické instalaci Eset Endpoint Antivirus na oba testovací klienty. Na klientech jsem ověřil instalaci pomocí otevření programu Eset Endpoint Antivirus. V programu můžeme zjistit stav aktualizací, pod jakou licencí je program spuštěn a další.



Obrázek 33. Kontrola dokončení instalace Eset Endpoint na koncové stanici

8 ŘEŠENÍ NEJČASTĚJŠÍCH PROBLÉMŮ V RÁMCI ESET PROTECT

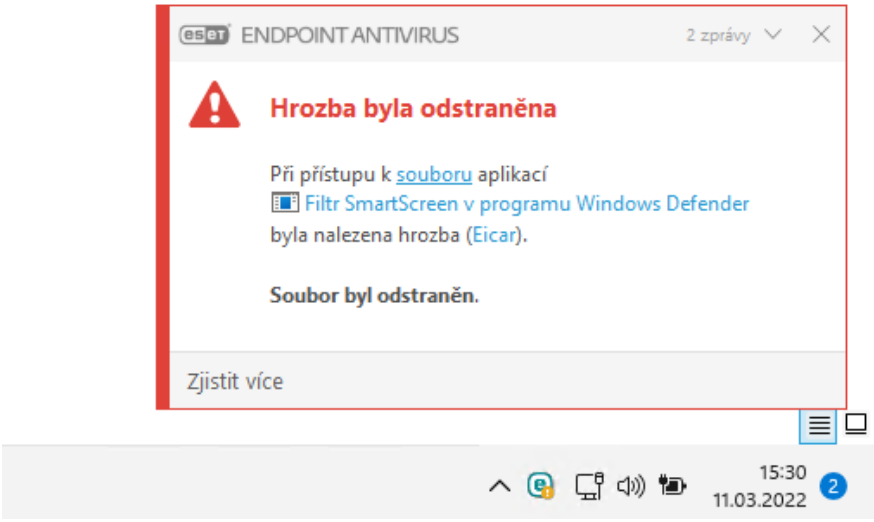
Eset nabízí širokou škálu možností pro správu klientských zařízení a řešení různých bezpečnostních problémů. V práci jsou popsány nejčastější úlohy, které může správce nástroje Eset Protect řešit. Jedná se o detekci viru na klientské stanici, odpojeni klienta od sítě, restart nebo vypnutí PC na dálku a další.

8.1.1 Detekce viru a práce s ním

Jednou s nejzákladnějších funkcí antiviru je zachycení virové hrozby.

Pro test detekce a ukázku záchytu potencionální hrozby na koncové stanici jsem využil testovacího souboru ze stránek eicar.org. [46]

Po spuštění souboru byl tento detekován jako hrozba. Proběhla akce vyléčení odstraněním a umístění souboru do karantény. Na obrázku níže můžete vidět vyskakovací okno programu Eset Endpoint Antivirus, na kterém je oznámení o detekci hrozby.

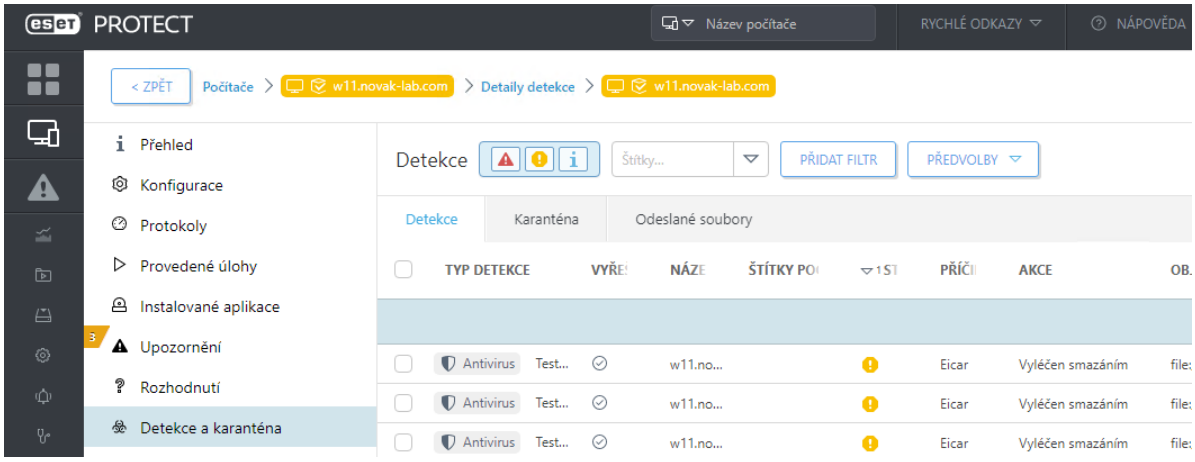


Obrázek 34. Ukázka detekce hrozby na koncové stanici

V rámci Eset Endpoint Antiviru na dané klientské stanici je možno zobrazit soubory v karanténě. Zde přehledně vidíme, že došlo k několika pokusům o spuštění daného souboru a vždy byla provedena příslušná akce a proběhnulo jeho umístění do karantény.

Obrázek 35. Detekované hrozby uložené do karantény na koncové stanici W11

Ihned po detekci hrozby na klientovi se tato přehledně zobrazí i v rámci portálu Eset Protect, kde můžeme vše přehledně prověřit. V případě, kdy máme nastaveno upozornění, tak je zaslána i automatická notifikace. Zvláště pokud by se jednalo o více výskytů na různých stanicích.

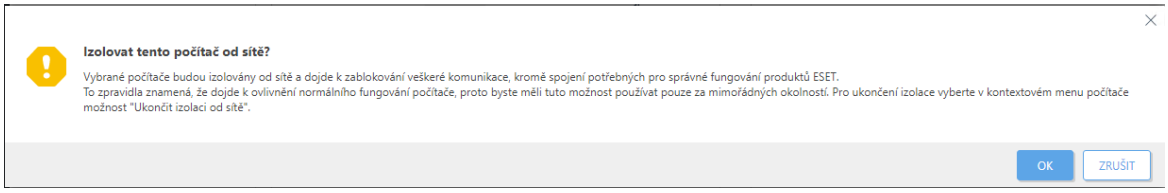


Obrázek 36. Ukázka detekce a karantény nebezpečného programu v Eset Protect

8.1.2 Izolace klienta od sítě

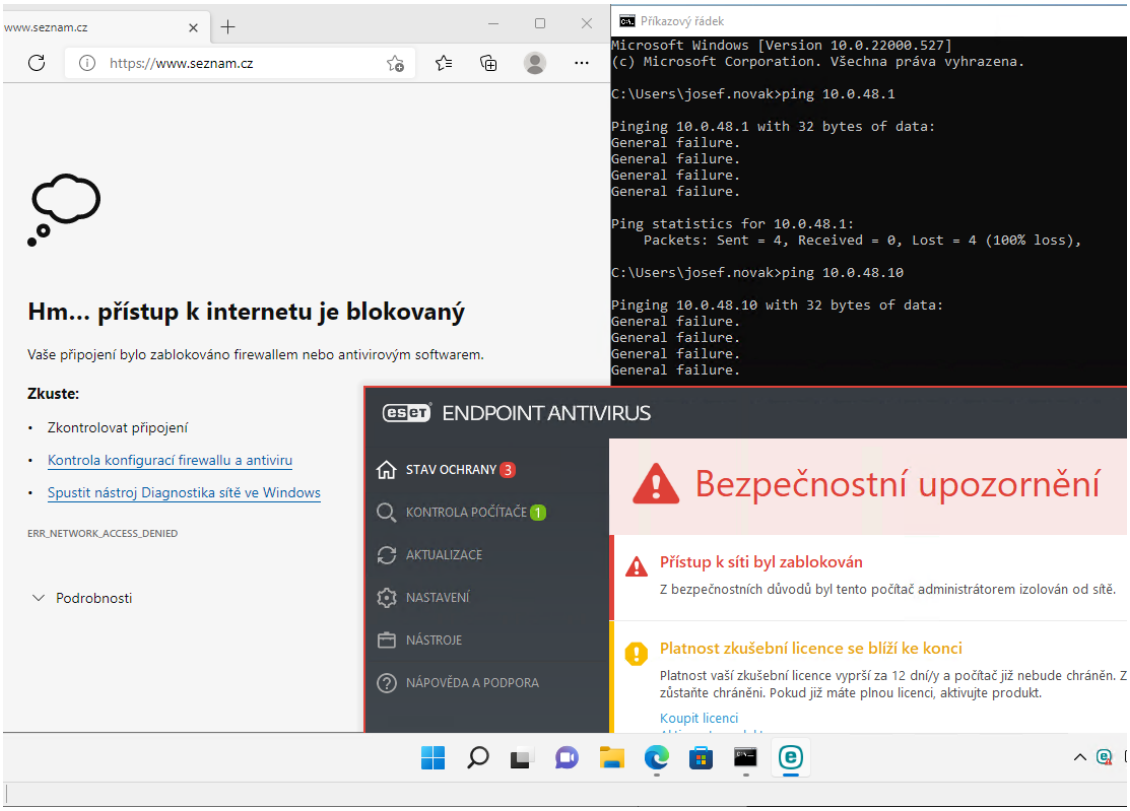
V případě napadení klienta virem, ransonwarem apod. je možno klienta okamžitě síťové izolovat. Buď na základě automatického pravidla nebo ručně. V tomto režimu se mimo vlastní stanici hrozba nedostane dále do sítě. Jediná povolená výjimka je pro Eset Agenta, kterým lze řídit další kroky.

Jestliže chceme klienta izolovat ručně, stačí si najet na jeho detaily v rámci Eset Protect a zvolit možnost „Izolace od sítě“. Následně stačí jen potvrdit.



Obrázek 37. Ukázka izolování klientské stanice od sítě

Po zapnutí funkce izolace dojde k odstřižení klientské stanice od okolní sítě. Jak vyplývá z obrázku níže, je zakázán provoz do internetu (otestováno pomocí přístupu na webovou stránku a taktéž pomocí příkazu ping na IP 8.8.8.8, což je DNS Googlu) a taktéž na okolní servery ve stejném adresním rozsahu (ověřeno pomocí příkazu ping na virtuální servery s IP 10.0.48.1 a 10.0.48.10). Zároveň Eset na klientské stanici hlásí status „Přístup k síti byl zablokován“.



Obrázek 38. Ukázka z koncové stanice po odpojení od sítě

Pro ukončení izolace od sítě stačí v nastrojí Eset Protect vybrat upozornění „Přistup k síti byl zablokován“ a zvolit možnost „Ukončit izolaci od sítě“. Ukončením izolace obnovíme předchozí funkční stav.

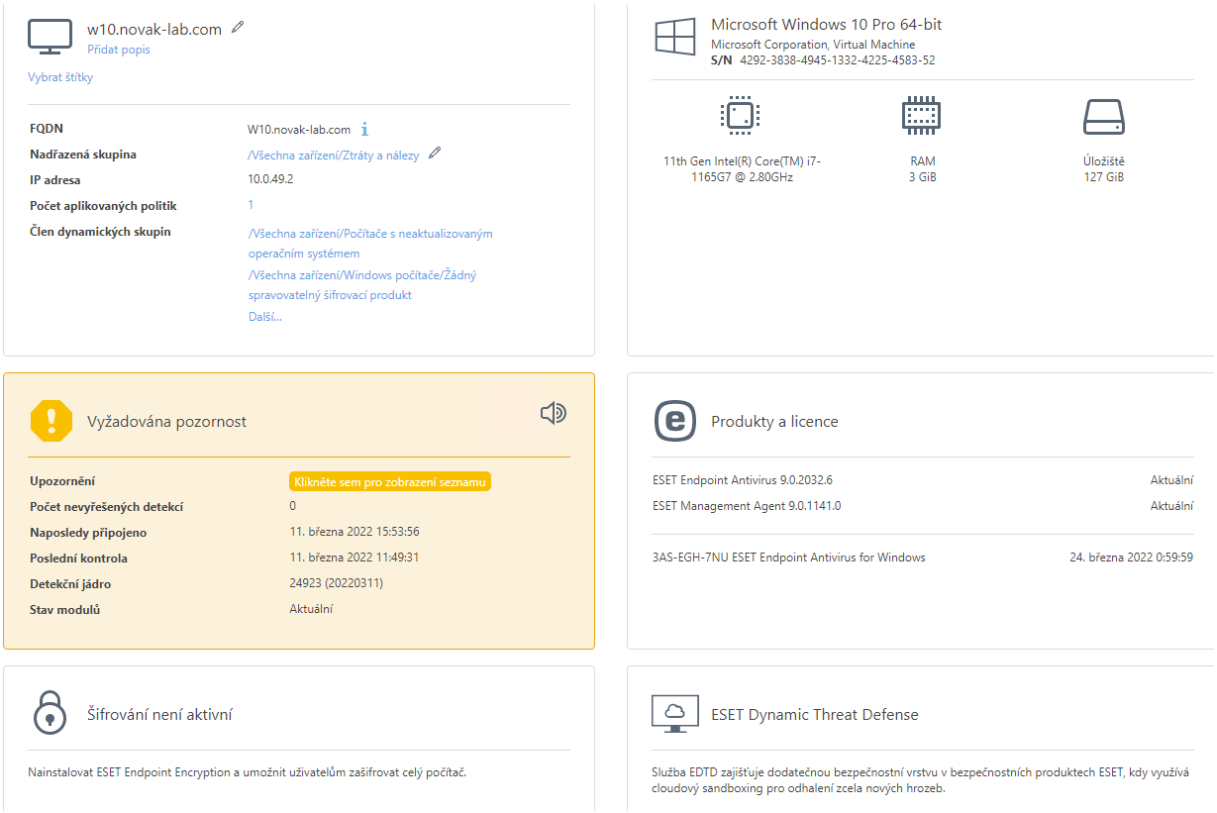
8.1.3 Zobrazení podrobností o daném klientu

Eset Protect nám nabízí celou řadu detailních informací o každém spravovaném zařízení. Tyto lze následně velmi rychle procházet a filtrovat.

Mezi informace, které lze zobrazit patří:

- hardwarová konfigurace (procesor, RAM, disk, grafická karta, síťové adaptéry, nainstalované tiskárny),

- název a verze operačního systému,
- plný doménový název počítače (FQDN) a jeho IP adresa,
- aktuálně přihlášený uživatel (dle tohoto lze i vyhledávat a najít PC na kterém je přihlášen požadovaný uživatel),
- přehled nainstalovaných aplikací (nejen Eset software),
- provedené úlohy z Eset Protect a jejich historie,
- detekce a karanténa na daném klientu.

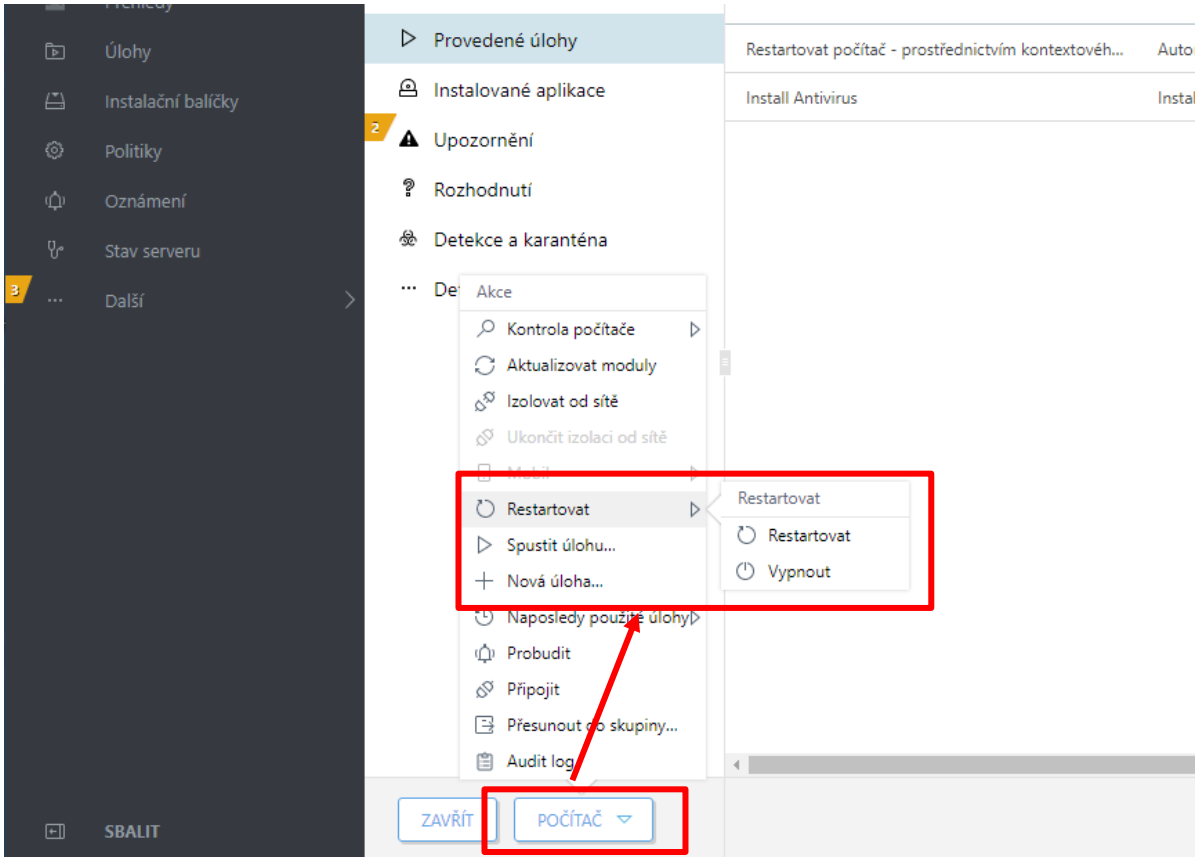


Obrázek 39. Výpis detailních údajů o klientské stanici v nástroji Eset Protect

8.1.4 Restart nebo vypnutí klienta

V situaci, kdy je kupříkladu kvůli aktualizacím, problému s aplikacemi apod. klientskou stanici nutné restartovat či vypnout, lze toto provést bez problémů vzdáleně.

Volbu nalezneme při zobrazení detailu koncové stanice, kterou chceme restartovat nebo vypnout. Následně z kontextové nabídky „Počítač“ vybereme možnost „Restartovat“ a zde si již jen zvolíme požadovanou akci.

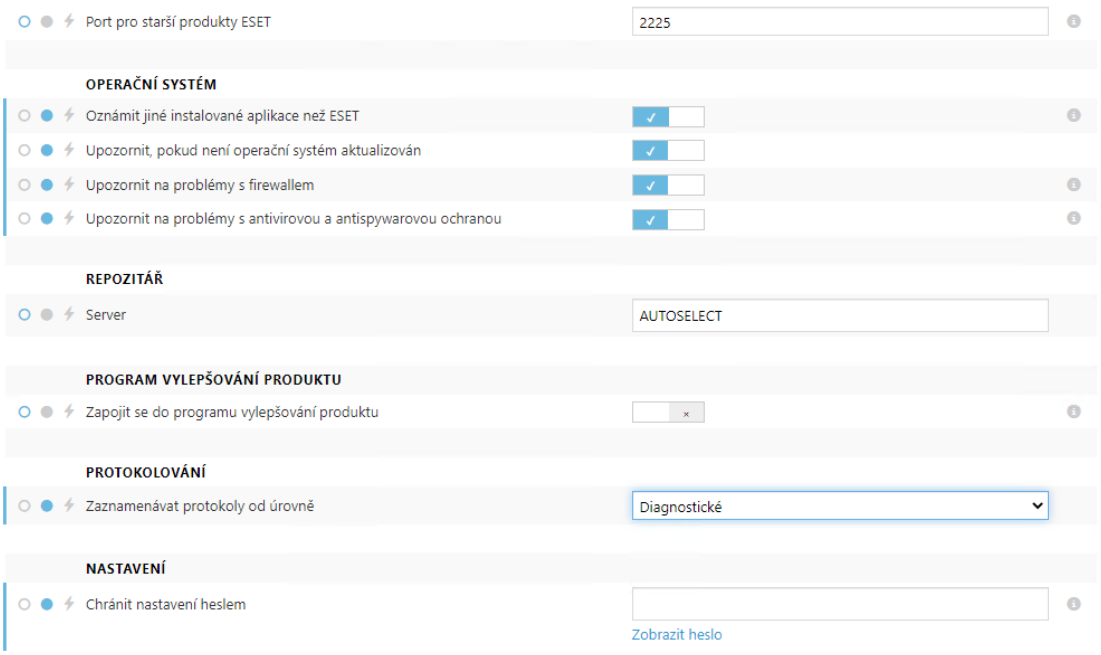


Obrázek 40. Ukázka vzdáleného restartu klienta

8.1.5 Politiky a jejich aplikování

V rámci výchozí instalace Eset Protect je vytvořeno velké množství předvolených bezpečnostních politik, které se dají snadno aplikovat. Můžeme volit mezi předdefinovanými politikami pro jednotlivé produkty (Eset Endpoint, Eset Full Disk Encryption, Eset Agent). Mezi jednotlivé politiky patří například Maximální ochrana, Doporučené nastavení, Zjistit všechny nainstalované programy a další. Tyto bezpečnostní politiky dopomáhají k požadovanému nastavení a správě produktů společnosti Eset. Zároveň pokud nám vyhovuje předdefinovaná politika, tak je její nasazení otázkou chvíle. Případně si politiku můžeme vytvořit sami na základě nejrůznějších požadavků a mnoha předvoleb, které se liší dle jednotlivých produktů.

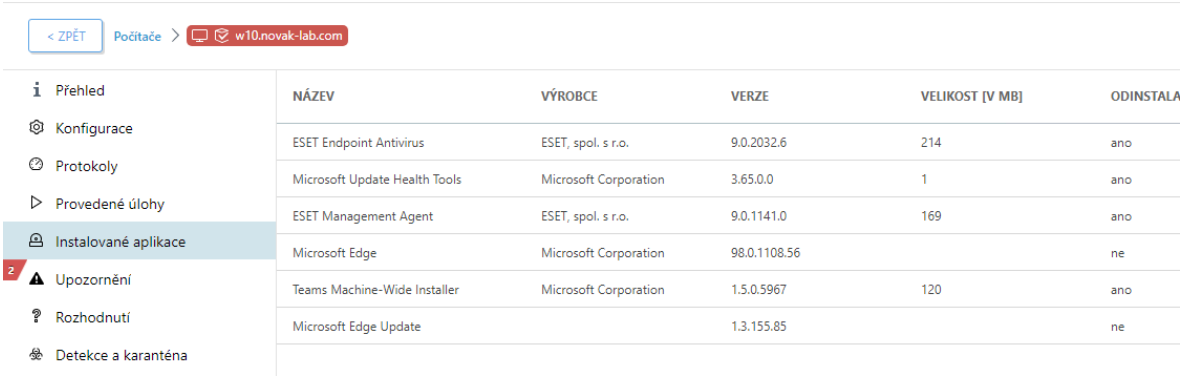
Na obrázku níže můžeme vidět část nastavení politiky pro Eset Agenta.



Obrázek 41. Vytvoření nové politiky – záložka nastavení

Politiku lze následně aplikovat jak pro jednotlivé zařízení, tak pro celé skupiny zařízení.

Případně po zapnutí politiky „Seznam aplikací – Zjistit všechny nainstalované aplikace“ lze zobrazit veškeré běžící aplikace na jednotlivých zařízení.



Obrázek 42. Přehled všech nainstalovaných aplikací na koncové stanici

8.1.6 Kontrola akcí a změn v audit logu

V rámci audit logu lze zobrazit veškeré akce a změny provedené všemi uživateli.

Lze využívat jednotlivých podrobných filtrů pro vyhledání specifických logů a následně je případně exportovat do několika formátů.

Přehled: Audit log

Název serveru
esmc2.novak-lab.com

Přehled vygenerován
18. března 2022 12:35:57 (UTC+01:00)

Počet záznamů
76

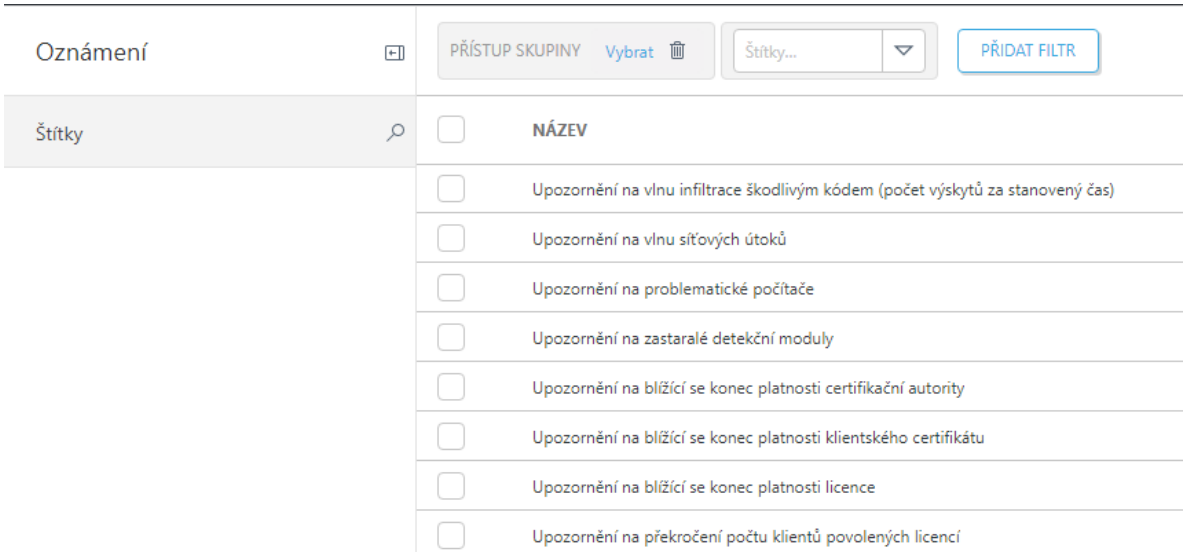
Filtry
Počet filtrů: 2

Čas výskytu	Typ	Akce	Detaily akce	Výsledek	Celé jméno u
18. března 2022 12:18:37	Serverová úloha	Start	Spuštění serverové úlohy 'Automaticky přejmenovat synchronizované počítače do FQDN formátu' typu 'Přejmenování počítačů'.	Úspěšné	Administrator
14. března 2022 14:34:10	Nativní uživatel	Odhlásit	Odhlášení nativního uživatele 'Administrator'.	Úspěšné	Administrator
14. března 2022 14:30:18	Dynamická skupina	Nastavit politiku	Přiřazení politiky 'Seznam aplikací – Zjistit všechny nainstalované aplikace' dynamické skupině 'Windows počítače', která se nachází ve skupině 'Všechna zařízení'.	Úspěšné	Administrator
14. března 2022 14:23:25	Serverová úloha	Start	Spuštění serverové úlohy 'Automaticky přejmenovat synchronizované počítače do FQDN formátu' typu 'Přejmenování počítačů'.	Úspěšné	Administrator
11. března 2022 16:25:08	Nativní uživatel	Odhlásit	Odhlášení nativního uživatele 'Administrator'.	Úspěšné	Administrator
11. března 2022 16:23:48	Podmínka spuštění klientské úlohy	Přiřadit	Přiřazení klientské úlohy 'VLC' počítači 'Všechna zařízení\Ztrátv a	Úspěšné	Administrator

Obrázek 43. Výpis jednotlivých akcí z audit logu

8.1.7 Správa oznámení

Součástí aplikace Eset Protect je i možnost spravovat různá oznámení. Upozornit je možno emailem, za pomoci SNMP trapu nebo jej uložit jen do syslogu. Již v základu je velké množství předvolených upozornění, které je možno využít.



Obrázek 44. Výběr přednastavených typů oznámení, které budou zasílány

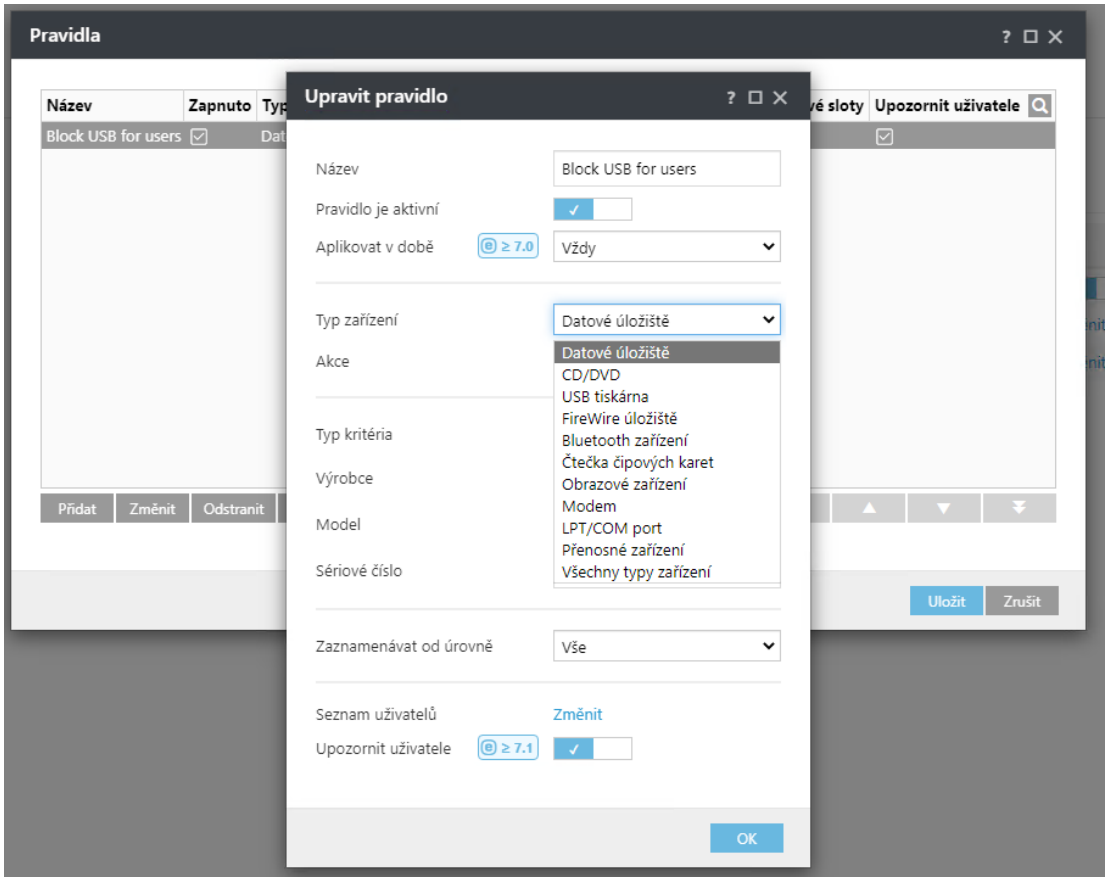
8.1.8 Zakázání USB uložiště na Windows klientu

Zablokování datového uložiště je možné přes politiky a funkci Správy zařízení, jenž obsahuje Eset Endpoint Antivirus.

Vytvoříme novou uživatelskou politiku s názvem „USB disable“, v nastavení politiky vybereme, že se má týkat nástroje Eset Endpoint for Windows a ve Správa zařízení vytvoříme pravidlo. Toto pravidlo bude obsahovat zapnutí položky Zapnout správu zařízení na kartě Obecné a v sekci Pravidla přes tlačítko změnit pravidlo definujeme.

Samotné omezení lze směřovat na nejrůznější typy zařízení, jako jsou CD/DVD, USB tiskárny anebo například Bluetooth zařízení.

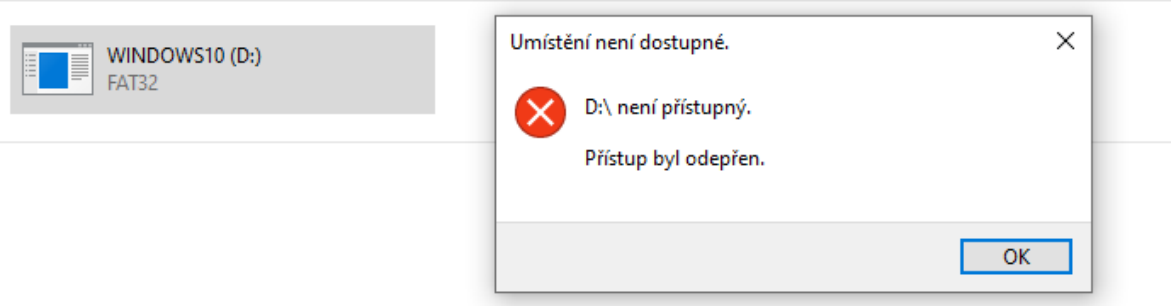
Jak vyplývá z obrázku níže, je zde zobrazeno okno pro upravu pravidla na blokování usb uložiště pro uživatele koncových klientských stanic. Je možné upravit dobu aplikování pravidla na určité časové rozmezí. Dále je zde možno vybrat typ zařízení z široké škály možností, v našem případě vybereme Datové uložiště. Další možností je úprava seznamu uživatelů, na které se bude pravidlo uplatňovat. Po restartu počítače (je nutno kvůli zapnutí funkce Správa zařízení) následně Eset blokuje veškeré přístupy na datové uložiště.



Obrázek 45. Okno pro upravení pravidla o zákazu USB

V programu Eset Endpoint Antivirus je možné zobrazit přehled pravidel, která jsou aplikována na klientskou stanici a provést tak kontrolu, že se korektně propsalo.

Po aplikování politiky na testovací stanici je již daný usb přenosný disk nedostupný a nedá se zobrazit. Na obrázku níže můžeme vidět hlášku, která se zobrazí při pokusu o přístup k usb přenosnému disku.



Obrázek 46. Hláška po připojení USB přenosného disku a následném pokusu o přístup k datům

8.1.9 Nastavení výjimek pro určité typy souborů nebo pro konkrétní umístění

Eset Protect umožňuje nastavení pravidel v rámci Antiviru. Je možno vynechat určitý typ souboru (například .iso, .bak) z rezidentní ochrany souborového systému nebo dát výjimku na dané umístění (například C:\Program Files\Hyper-V). Toto může být vhodné ve specifických případech, například na SQL serveru nechceme omezovat výkon a kontrolovat jeho soubory databáze a logů nebo temp souborů.

8.2 Závěrečné shrnutí

Praktická část je zaměřena na instalaci bezpečnostního balíčku od firmy Eset. Úvod se věnuje testovacímu prostředí, ve kterém byl bezpečnostní balíček nasazen. Testovací prostředí věrně simuluje firemní doménové prostředí a umožňuje nám otestovat funkcionalitu daného softwaru. Následně je uveden postup nasazení Eset Appliance pod hypervisorem Hyper-V a popsána její prvotní konfigurace. V navazující kapitole je uveden postup od samotného přirazení licence až po instalaci antivirového řešení na koncové stanice. Následně jsou analyzovány nejběžnější situace, které můžeme za pomoci nástrojů Eset řešit. Mezi tyto situace jsem vybral například detekci viru, vzdálené vypnutí nebo restart počítače, izolaci počítače od sítě nebo blokování USB datových uložišť.

ZÁVĚR

Bakalářská práce byla zaměřena na nasazení bezpečnostní balíčku od společnosti Eset. Cílem práce byl popis nasazení bezpečnostního balíčku Eset ve firemním doménovém prostředí a jednotlivých možností, které nabízí.

V úvodu teoretické části byly vysvětleny pojmy spojené s doménovým prostředím a virtualizací. Následně teoretická část pokračuje kapitolou o počítačové bezpečnosti, jež je v dnešní době stále více podstatným tématem a měla by na ni být upřena pozornost. Byly zde rozebrány některé nebezpečí, které hrozí každému uživateli počítačové techniky. Najdeme zde hrozby v podobě škodlivého softwaru a také podvodné praktiky, které útočníci využívají pro zisk citlivých údajů od uživatelů. Dále je zde věnována pozornost obraně proti těmto hrozbám, přičemž je zde zásadní skutečnost, že nejlepší obranou je volba vhodného softwarového řešení a také školení koncových uživatelů. V poslední části byl přiblížen vybraný bezpečnostní balíček od společnosti Eset. Byly zde rozebrány jeho části, hardwarové požadavky a provedeno srovnání s konkurencí.

Praktická část byla zaměřena na samotné nasazení bezpečnostního balíčku od společnosti Eset. V první části bylo popsáno testovací prostředí, které bylo zapotřebí vytvořit pro simulaci reálného prostředí firmy. Po vytvoření testovacího prostředí bylo přistoupeno k samotné instalaci bezpečnostního balíčku. Je zde popsána instalace ve virtuálním prostředí pomocí Hyper – V. Po úspěšné instalaci byla provedena konfigurace pomocí webové konzole. Prvním krokem bylo přiřazení testovací licence. Dále instalace Eset agenta na koncové stanice za pomoci skupinových politik. Po kontrole úspěšného nasazení agenta na koncových stanicích bylo přistoupeno k instalaci Endpoint. Závěr praktické části byl věnován testování nejběžnějších bezpečnostních problémů. Následoval test detekce virové hrozby, který proběhl úspěšně. Poté bylo přistoupeno k testování dalších funkcí nástroje Eset Protect. Bylo otestováno odpojení koncové stanice od sítě, odpojení USB datového uložiště a další.

SEZNAM POUŽITÉ LITERATURY

[1] STANEK, William R. Microsoft Windows Server 2012: kapesní rádce administrátora. Brno: Computer Press, 2015. ISBN 978-80-251-3817-5.

[2] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 4., aktualiz. a rozš. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2073-6.

[3] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[4] Qu'est-ce que le DNSSEC ?. HOSTEUR [online]. 2019 [cit. 2022-05-12]. Dostupné z: https://www.hosteur.com/ressources/articles/fonctionnement-service

[5] What is DHCP protocol and how does it work?. GRANDMETRIC [online]. 2017 [cit. 2022-05-12]. Dostupné z: https://www.grandmetric.com/2017/07/18/what-is-dhcp-and-how-does-it-work/

[6] Active Directory komponenty - domain, tree, forest, site. SAMURAJ-cz [online]. 2008 [cit. 2022-05-12]. Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/

[7] Applying Group Policy. Microsoft [online]. [cit. 2022-05-12]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/applying-group-policy

[8] Group Policy Objects. Microsoft [online]. 2018 [cit. 2022-05-12]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects

[9] Group Policy - řízení aplikace politik. SAMURAJ-cz [online]. 2010 [cit. 2022-05-12]. Dostupné z: https://www.samuraj-cz.com/clanek/group-policy-rizeni-aplikace-politik/

[10] Co je virtualizace?. Azure [online]. c 2022 [cit. 2022-05-12]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-virtualization/

[11] Co je virtuální počítač?. Azure [online]. c 2022 [cit. 2022-05-12]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-a-virtual-machine/#overview

[12] Úvod do virtualizace na desktopu. Michal Zobec: Virtuální PC Blog [online]. 2014 [cit. 2022-05-12]. Dostupné z: https://www.virtualnipc.cz/vmware-workstation-uvod-do-virtualizace-na-desktopu-1875

[13] Počítačová bezpečnost (Computer security). MANAGEMENT MANIA [online]. c 2011-206 [cit. 2022-05-12]. Dostupné z: https://managementmania.com/cs/pocitacova-bezpecnost

[14] CO TO JE MALWARE. Internet BEZPEČNĚ [online]. C 2018 [cit. 2022-05-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/

[15] POČÍTAČOVÉ VIRY, ČERVI A TROJSKÉ KONĚ. Internet BEZPEČNĚ [online]. c 2018 [cit. 2022-05-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[16] Co je to Makro vir?. IT SLOVNÍK [online]. c 2008-2022 [cit. 2022-05-12]. Dostupné z: https://it-slovnik.cz/pojem/makro-vir

[17] Červ. Počítačové viry [online]. c 2021 [cit. 2022-05-12]. Dostupné z: https://viry.estranky.cz/clanky/cerv.html

[18] Červ. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/glossary/cs-CZ/worms.html

[19] Trojský kůň. ESET [online]. c 1992–2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/trojsky-kun/

[20] Trojský kůň. ESET [online]. c 1992–2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/glossary/cs-CZ/trojan_horses.html

[21] Spyware. ESET [online]. c 1992–2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/spyware/

[22] Spyware. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/glossary/cs-CZ/spyware.html

[23] Ransomware. ESET [online]. c 1992–2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/ransomware/

[24] RANSOMWARE. Internet BEZPEČNĚ [online]. c 2018 [cit. 2022-05-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/ransomware/

[25] Ransomware. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/glossary/cs-CZ/ransomware.html

[26] Adware. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/adware/

[27] Adware. Avast [online]. c 1988-2022 [cit. 2022-05-12]. Dostupné z: https://www.avast.com/cs-cz/c-adware

[28] Adware. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/glossary/cs-CZ/adware.html

[29] CO JE TO PHISHING. HOAX.cz [online]. c 2000-2020 [cit. 2022-05-12]. Dostupné z: https://www.hoax.cz/phishing/co-je-to-phishing

[30] Phishing. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/phishing/

[31] What Is Pharming and How to Protect Yourself. Kaspersky [online]. c 2022 [cit. 2022-05-12]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[32] Co je Pharming?. SSL.com [online]. 2021 [cit. 2022-05-12]. Dostupné z: https://www.ssl.com/cs/blogy/co-je-pharming/#ftoc-heading-1

[33] Antivirus. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/antivirus-software/

[34] Firewall. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://www.eset.com/cz/firewall/#co-je-hardware-firewall

[35] Představení ESET PROTECT. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/protect_admin/90/cs-CZ/

[36] ESET Enterprise Inspector. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/eei/1.6/en-US/

[37] Hardware. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/protect_smb/90/cs-CZ/hardware.html

[38] Podporovaná Desktop Provisioning prostředí. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/protect_install/80/cs-CZ/supported_desktop_provisioning_environments.html

[39] Představení ESET PROTECT Cloud. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/protect_cloud/cs-CZ/index.html

[40] Rozdíly mezi on-premise a cloudovou konzolí pro vzdálenou správu. ESET [online]. c 1992-2022 [cit. 2022-05-12]. Dostupné z: https://help.eset.com/protect_cloud/cs-CZ/differences_onprem_cloud.html

[41] The Top 10 Antivirus Software For Small Businesses. Expert Insight [online]. c 2022 [cit. 2022-05-14]. Dostupné z: https://expertinsights.com/insights/top-10-antivirus-software-for-small-businesses/#ESET%20Endpoint%20Security

[42] Sandbox. DIGITÁLNÍ PEVNOST [online]. c 2018 [cit. 2022-05-18]. Dostupné z: https://www.digitalnipevnost.cz/viki/sandbox

[43] What is a zero-day exploit?. Norton [online]. c 2019 - 2022 [cit. 2022-05-18]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html

[44] Download ESET PROTECT. ESET [online]. c 1992-2022 [cit. 2022-05-18]. Dostupné z: https://www.eset.com/int/business/download/eset-protect/#virtual

[45] Deploy the ESET Management Agent using a Group Policy Object (GPO). ESET [online]. c 1992-2022 [cit. 2022-05-18]. Dostupné z: https://support.eset.com/en/kb6864-deploy-the-eset-management-agent-using-a-group-policy-object-gpo

[46] ANTI MALWARE TESTFILE. Eicar [online]. [cit. 2022-05-18]. Dostupné z: https://www.eicar.org/download-anti-malware-testfile/

[47] Meet Pharming - The New Old Kid on the Block. SOS Daily News [online]. 2017 [cit. 2022-05-18]. Dostupné z: https://sosdailynews.com/news.jspx?articleid=%20B39F74F035EA82E9100C308D648D6BFF

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory.
DNS	Domain Name System.
DHCP	Dynamic Host Configuration Protocol.
ACL	Access Control List
DC	Domain Controller
AD CS	Active Directory Certifikace Services.
AD DS	Active Directory Domain Services.
GPO	Group policy object.
URL	Uniform Recource Locator.
OU	Organizational unit.
IT	Information technology.
IP	Internet Protocol.
RD	Rogue Detector.
OS	Operating System.
SQL	Structured Query Language
IO	Input/Output
SSD	Solid state drive.
HDD	Hard Disk Drive.
RAM	Random – acess memory.
IOPS	Input/Output operation per second
HW	Hardware.
VPN	Virtual Private Network.

LAN	Local Area Network.
SNMP	Simple Network Management Protocol
FQDN	Fully Qualified Domain Name
CD	Compact Disc
USB	Universal Serial Bus.
DVD	Digital Video Disc.
HTTPS	Hypertext Transfer Protocol Secure

SEZNAM OBRÁZKŮ

SEZNAM TABULEK