(**Au**tomated **To**ol **for Se**curity **S**ettings)

1. Instalace nástroje

Archiv skript.zip je nutné rozbalit do předem vytvořené složky C:\nukib, z jiného umístění by skript nebyl funkční.

Archiv obsahuje dva soubory:

- prislo-od-nukib – obsahuje pomocné soubory pro běh skriptu,
- prave-tlacitko-spustit-jako-spravce.bat – skript samotný.

Tak jak název napovídá, je nutné skript spouštět s oprávněním správce (administrátora), tj. pod účtem správce, a ještě zvolit možnost – Spustit jako správce.

1.1. Minimální softwarové předpoklady pro spuštění skriptu

Operační sytém Windows 10: Pro, Enterprise, Education (64 bit) 21H1, build 19043. (Minimálně, ale nezaručeně od buildu 17063.)
Pokud vaše organizace využívá vlastní, upravené, případně automatizované nástroje pro instalaci operačních systémů, pak je pro instalaci počítače, který má být certifikován nepoužívejte.

2. Nastavení OS

Nástroj provádí kompletní nastavení OS podle bezpečnostní dokumentace kapitoly Bezpečnostní nastavení operačního systému MS Windows. Dále jsou citovány položky z této kapitoly. Položky uvedené v článku 2.1 jsou nastaveny bez možnosti úpravy nastavení.
Položky uvedené v článku 2.2 může uživatel pomocí nástroje změnit dočasně nebo trvale.

2.1. Nedovolí úpravu uživatelem a nastavuje:

(T24) Povolit instalaci zařízení s těmito identifikačními čísly zařízení
Default: ---
NÚKIB: **Zakázat** / povolit

(T35) (T36) Disketové jednotky: Odepřít oprávnění ke čtení / zápisu
Default: ---
NÚKIB: **Povoleno** / zakázáno

(T40) Všechny třídy vyměnitelného úložiště: Odepřít veškerá oprávnění
Default: ---
NÚKIB: Povoleno / **zakázáno**

(T43) (T44) Páskové jednotky: Odepřít oprávnění ke čtení / zápisu
Default: ---
NÚKIB: **Povoleno** / zakázáno

(T45) (T46) Zařízení WPD: Odepřít oprávnění ke čtení / zápisu
Default: ---
NÚKIB: **Povoleno**

2.2. Dovolí úpravu uživatelem (trvale nebo dočasně):

(002) Maximální stáří hesla
Default: 42
NÚKIB varianta 1: 90 dnů
NÚKIB varianta 2: 730 dnů

(003) Minimální délka hesla
Default: 0 znaků
NÚKIB varianta 1: uživatelský účet 9 znaků, (administrátorský účet 12 znaků)
NÚKIB varianta 2: uživatelský účet 12 znaků, (administrátorský účet 14 znaků)

(008) Prahová hodnota pro uzamčení účtu
Default: 0 chybných pokusů o přihlášení
NÚKIB varianta 1: 3 chybné pokusy
NÚKIB varianta 2: 7 chybných pokusů
U položek (002), (003) a (008) může uživatel zvolit variantu 1 nebo 2, kombinace variant u jednotlivých položek není možná.

(T26) Zakázat instalaci vyměnitelných zařízení
Default: ---
NÚKIB: **Povolit** / Zakázat
Tato položka je měněna volbou 5 v menu skriptu, a to jen dočasně pro skriptem řízené přidání dalšího USB disku.

(T27) Zakázat instalaci zařízení nepopsaných v jiných nastaveních zásad
Default: ---
NÚKIB: **Povolit** / Zakázat (v souladu s bezpečnostní politikou IS)
Tato položka je měněna volbou 7 v menu skriptu, a to jen dočasně pro skriptem řízené přidání dalšího USB zařízení (myš, klávesnice, …)

(T30) (T31) Disk CD a DVD: Odepřít oprávnění ke čtení / zápisu
Default: ---
NÚKIB: **Povoleno** / zakázáno (v souladu s bezpečnostní politikou IS)
Po na nastavení skriptem povoleno, ale je možné volbou 3 v menu skriptu změnit trvale na **zakázáno**. Položky (T30) a (T31) se mění společně, není možné nastavit samostatně.

(T38) (T39) Vyměnitelné disky: Odepřít oprávnění k zápisu / čtení
Default: ---
NÚKIB: **Povoleno** / zakázáno
Po nastavení skriptem povoleno, ale je možné volbou 4 v menu skriptu změnit trvale na **zakázáno**. Položky (T38) a (T39) se mění společně, není možné nastavit samostatně.

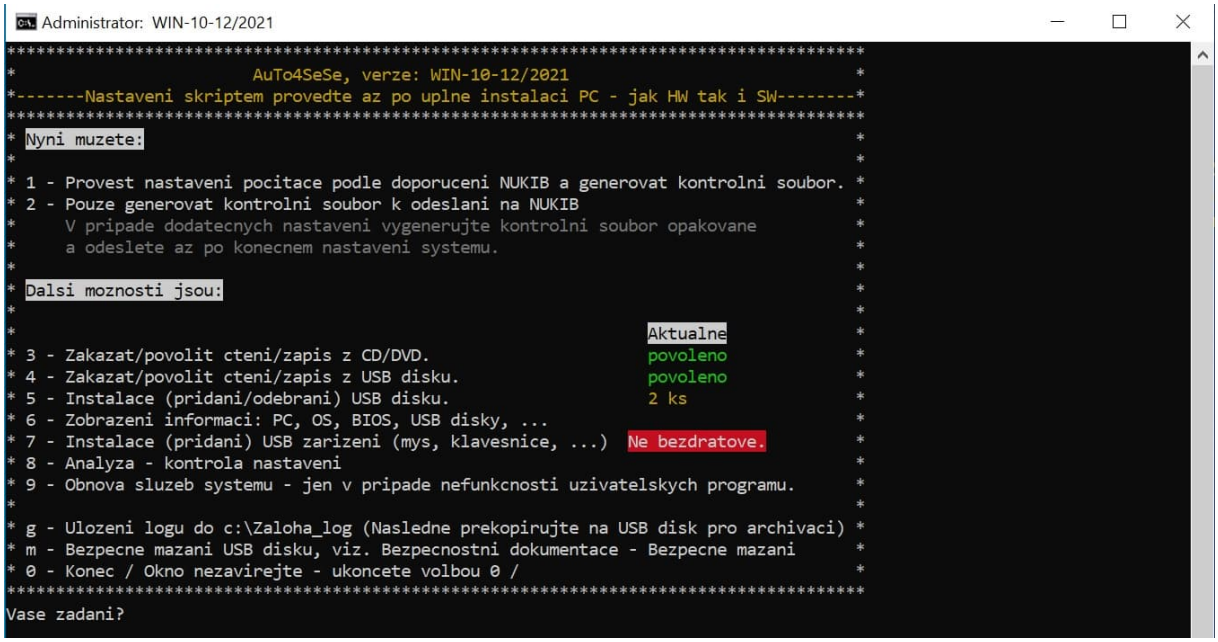
3. Práce se skriptem

Možnosti skriptu můžeme rozdělit na tři základní úrovně:

a) Nastavení systému podle doporučení výše jmenovaného dokumentu

b) Dodatečné nastavení – úpravu nastavení

c) Kontrolu a generování souborů k posouzení nastavení pro NÚKIB



Základní obrazovka skriptu

3.1. Nastavení systému

Systém nastavujte až po kompletní instalaci systému, HW příslušenství i uživatelského SW.

Nastavení systému se provádí volbou 1. Následuje:

- informace o zálohování nastavení služeb systému,
- smazání nepotřebných aplikací integrovaných do systému,
- **dotaz** na volbu politiky hesel,
- informace o tom, že všichni uživatelé budou muset při dalším přihlášení změnit heslo,
- **dotaz** na povolení nebo zakázání v systému vestavěného účtu správce (admin_root),

Pro malé systémy se sloučenou funkcí provozního a bezpečnostního správce doporučujeme tento účet povolit. Při povolení účtu je vygenerováno silné heslo, které s názvem účtu zapište a uložte v trezoru. Heslo není utajovanou informací ve smyslu zákona č. 412/2005 Sb., ale musí být chráněno jako utajovaná informace takového stupně utajení jako je stupeň utajení informací, ke kterým umožní přístup.

- **dotaz** na povolení čtení a zápisu z CD/DVD,
- **dotaz** na povolení čtení a zápisu z USB disku,
- při povolení zápisu a čtení z USB – **dotaz** na okamžité nebo odložené přidání USB disků do systému,

Skript ze systému odebral všechny dříve vložené USB disky a nyní nebo později musíte pomocí skriptu disky opět přidat (nainstalovat). Jinak žádný USB disk nebude funkční.

Nyní se předpokládá, že používáte k přenosu skriptu do nastavovaného počítače USB disk, který budete následně využívat, a proto ho do systému můžete přidat.

- **dotaz** na přidání dalšího USB disku,
- držte se pokynů skriptu a přidejte nyní nebo později všechny USB disky,

Veškeré USB disky, které budou v systému přidány, musí být evidovány. Pro instalace SW, aktualizace, … zaevidujte a používejte výlučně neutajovaný USB disk.

- informace o generování kontrolního souboru.

Soubory odeslat-nastaveni.txt a odeslat-hash.txt byly vygenerovány do složky C:\nukib. Pokud tímto vaše nastavení počítače skončilo, pak soubory odeslat-nastaveni.txt a odeslat-hash.txt odešlete datovou schánkou, ISDN: zzfnkp3 společně s dokumentací k vašemu systému na NÚKIB. Ale pokud budete provádět další nastavení – povolovat čtení zápis CD/DVD/USB, přidávat USB disky nebo USB zařízení, tak jsou tyto soubory smazány a je nutné je vygenerovat znovu volbou 2.

3.2. Dodatečné nastavení

Pro dodatečné nastavení jsou k dispozici volby:

3 - Můžete zakázat/povolit čtení/zápis z CD/DVD – toto nastavení je trvalé (do další změny) a musí se shodovat s dokumentací k vašemu systému.

4 - Můžete zakázat/povolit čtení/zápis z USB disku – toto nastavení je trvalé (do další změny) a musí se shodovat s dokumentací k vašemu systému.

V některých případech, ale v souladu s dokumentací může správce systému povolit čtení/zápis jen dočasně, například pro účely aktualizace SW, …

5 - Instalace (přidání) dalšího, dalších USB disků nebo odstranění všech disků, které jsou v systému přidány. Toto nastavení je dočasné, dovolí přidat USB disk jen, když je spuštěno.

Skript umožňuje přidávat jednotlivé disky, ale případně odstraňuje veškeré disky najednou. Při nutnosti odstranění USB disku, je pak potřeba zbylé USB disky, které mají být v systému, přidat opět jednotlivě.

7 - Instalace (přidání) dalšího, dalších USB zařízení, které budete v systému využívat. Toto nastavení je dočasné, dovolí přidat USB zařízení jen, když je spuštěno.

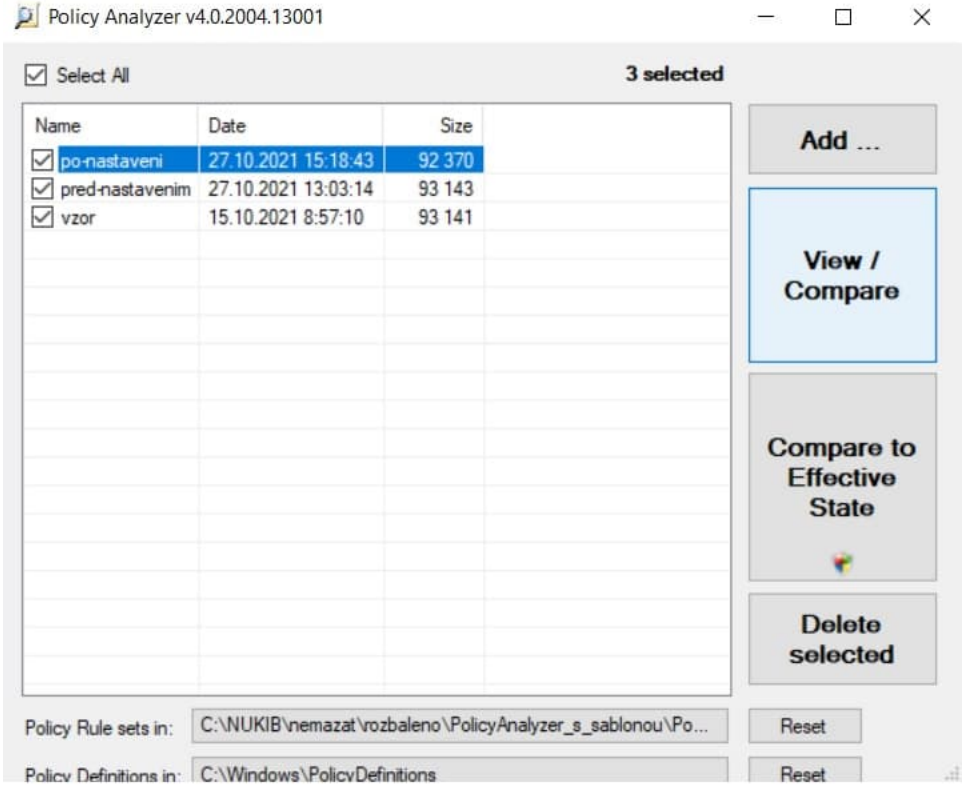
Po nastavení skript blokuje přidání dalších USB zařízení. Pokud chcete do systému přidat další USB zařízení, které není uvedené ve schválené dokumentaci, tak si nejdříve vyžádejte souhlas NÚKIB.

m – umožňuje bezpečné mazání vyjímatelných disků připojitelných prostřednictvím USB rozhraní. Není možné použít pro snížení stupně utajení média, vyjma případů popsaných v bezpečnostní dokumentaci sytému.

g – provede zálohu bezpečnostního, aplikačního a systémového logu do složky C:\Zaloha_log a následně obsah těchto logů v počítači smaže. Proveďte archivaci logů na USB disk.

3.3. Kontrola

Pro kontrolu slouží volba 8, která spustí Policy Analyzer a je možné porovnat aktuální a doporučené nastavení. Za předpokladu, že proběhlo nastavení systému pomocí skriptu, bude možné porovnat 3 nastavení („po-nastaveni“, „pred-nastavenim“ a „vzor“).



PolicyAnalyzer

Po výběru nastavení, která mají být porovnávána a volbě „View/Compare“ je k dispozici výstup, kde jsou rozdílné položky podbarveny žlutě nebo šedě, které v nastavení chybí.

Některé rozdíly v nastaveních (porovnáváme „po-nastaveni“ a „vzor“), jsou přípustné, a to za předpokladu, že byl systém nastaven ručně pomocí gpedit.msc. Například položka porovnávající oznámení, že uživatel přistupuje do utajovaného systému – zde musí být zachován význam, ale nemusí se na 100 % shodovat se „vzor“.

Naproti tomu například logování, minimální velikost logovacího souboru, … musí být totožné se „vzor“.

U délky, doby platnosti a počtu chybných pokusů u hesla musí přesně odpovídat jedné ze dvou variant (9/90/3 nebo 12/730/7), vzor uvádí 12/730/7, ale 9/90/3 ve výstupu „po-nastaveni“ není tedy chybou, byť bude žlutě podbarveno. Stejné platí i pro čtení/zápis u CD/DVD a USB – konečné nastavení musí odpovídat dokumentaci systému a může se od „vzor“ lišit.

4. Odeslání kontrolních souborů

Po ukončení nastavení, kdy je systém ve stavu, ve kterém bude užíván vygenerujte kontrolní soubory (volba 2 v menu skriptu) odeslat-nastaveni.txt a odeslat-hash.txt Soubory odešlete datovou schánkou, ISDN: zzfnkp3 společně s dokumentací k vašemu systému.