Application whitelisting

ako efektívna ochrana pred škodlivým kódom

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Do vašej organizácie prišiel phishingový e-mail na niekoľko e-mailových kont zamestnancov. Prezentoval sa ako informácia od dodávateľa a v prílohe obsahoval súbor cenova_ponuka.pdf.exe. Niektorí príjemcovia si hrozbu všimli a e-mail ignorovali alebo zmazali. Dvaja však riziko nepostrehli, stiahli a spustili škodlivý súbor, ktorý započal proces šifrovania ...

Čo je application whitelisting

V praxi dochádza k situáciám, keď používatelia nahrávajú do verejných Application whitelisting je účinná metóda, ktorá poskytuje významné zvýšenie ochrany operačných systémov Windows voči malvéru. Jej nasadenie zabráni vykonaniu akéhokoľvek spustiteľného súboru, ktorý nebol vopred schválený. To znamená, že aj keď zlyhá antimalvérové riešenie a používateľ úspešne stiahne infikovaný alebo škodlivý spustiteľný súbor alebo skript do svojho zariadenia, nepodarí sa mu jeho obsah vykonať.

Antivírus, resp. antimalvérové riešenia fungujú najmä na princípe blacklistingu, teda povolia spustiť všetko, čo nie je zakázané, resp. neobsahuje zakázané signatúry. To umožňuje novým, neznámym a vhodne upraveným vzorkám malvéru ľahko preniknúť do vašej infraštruktúry. Application whitelisting prináša opačný prístup, ktorý je výrazne bezpečnejší. Povolí spustiť len to, čo sa explicitne nachádza na zozname a všetko ostatné zakáže.

Kedy používať whitelisting aplikácií

Tento prístup je optimálny, keď spravujeme pracovné stanice zamestnancov, ktorí majú rovnaké pracovné potreby, resp. používajú rovnaké softvérové vybavenie. Môže sa jednať o skupiny zariadení s rovnakým „golden image".

Údržba, aktualizácia a testovania zoznamu povolených spustiteľných súborov v infraštruktúre, kde je zapojených veľa pracovných staníc so vzájomne odlišnou, resp. unikátnou softvérovou výbavou, môže byť náročná. Rovnako môže byť náročné udržiavať zoznam a testovať pre a častou zmenou softvérového vybavenia. Príkladom sú zariadenia developerov, kde dochádza prirodzene k častej inštalácii nástrojov a knižníc a zmene spustiteľných súborov vyvíjaných aplikácií, vzhľadom na kompiláciu ich nových verzií.

Použitie application whitelistingu vám zdarma a bez potreby inštalácie dodatočného softvéru poskytne zvýšenú ochranu a doplnenie schopností vášho antivírusového riešenia. Ak používate riešenia typu EDR/XDR, funguje ako doplnková vrstva ochrany medzi antivírusom a EDR/XDR.

Vytvorenie zoznamu hashov povolených spustiteľných súborov

V prvom rade potrebujeme vytvoriť zoznam aplikácií, resp. spustiteľných súborov, ktoré chceme používateľom povoliť.

V konzole Command Prompt vyhľadajte všetky spustiteľné súbory v systéme

```
dir c:\*.exe /a /s /b >> zoznam.txt
```

Zobrazí všetky súbory s príponou EXE prítomné na disku C, vrátane skrytých a systémových súborov (/a), rekurzívne vo všetkých podzložkách danej zložky (/s), vo forme zoznamu bez dodatočných informácií (/b).

```
for /F "delims=" %p in (c:\list.txt) do certutil -hashfile "%p" SHA1 >> hashes.txt
```

Prečíta súbor list.txt a vezme z neho cesty ku jednotlivým nájdeným súborom. Parameter "delims=" zabezpečí, že názvy súborov obsahujúce medzery ostanú nerozdelené. Následne nástroj certutil vypočíta hashe SHA1 pre každý súbor a zapíše výsledky do súboru hashes.txt.

Ak chceme uložiť do výstupu iba samotné hashe, môžeme použiť napríklad nasledujúci príkaz. Funkcia „find /V „:“ “ vypíše všetky riadky, ktoré neobsahujú reťazec v úvodzovkách (pre nás dvojbodku).

```
for /F "delims=" %p in (c:\list.txt) do
      (certutil -hashfile "%p" SHA1 | find /V “:”) >> hashes.txt
```

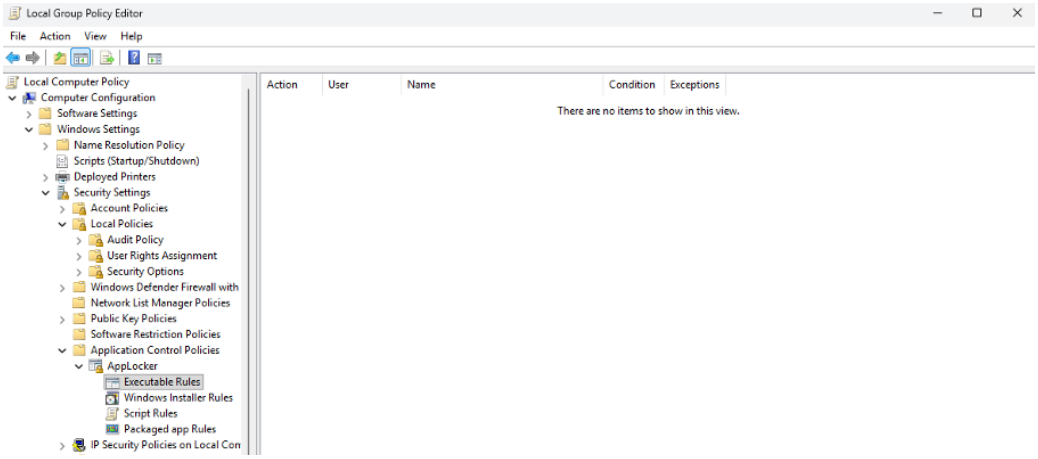
Rovnaký postup použijeme pre vytvorenie whitelistu skriptov (ps1, bat, vbs, js, ...).
Náš nový whitelist bude správne fungovať, až dokiaľ nevykonáme aktualizáciu niektorej legitímnej aplikácie. Vtedy sa zmení hash prislúchajúcich spustiteľných súborov v zozname a bezpečnostné pravidlá nedovolia novú verziu spustiť. Preto je potrebné whitelist priebežne aktualizovať, resp. dbať o to, aby obsahoval aktuálne hashe pre každú žiadanú aplikáciu.

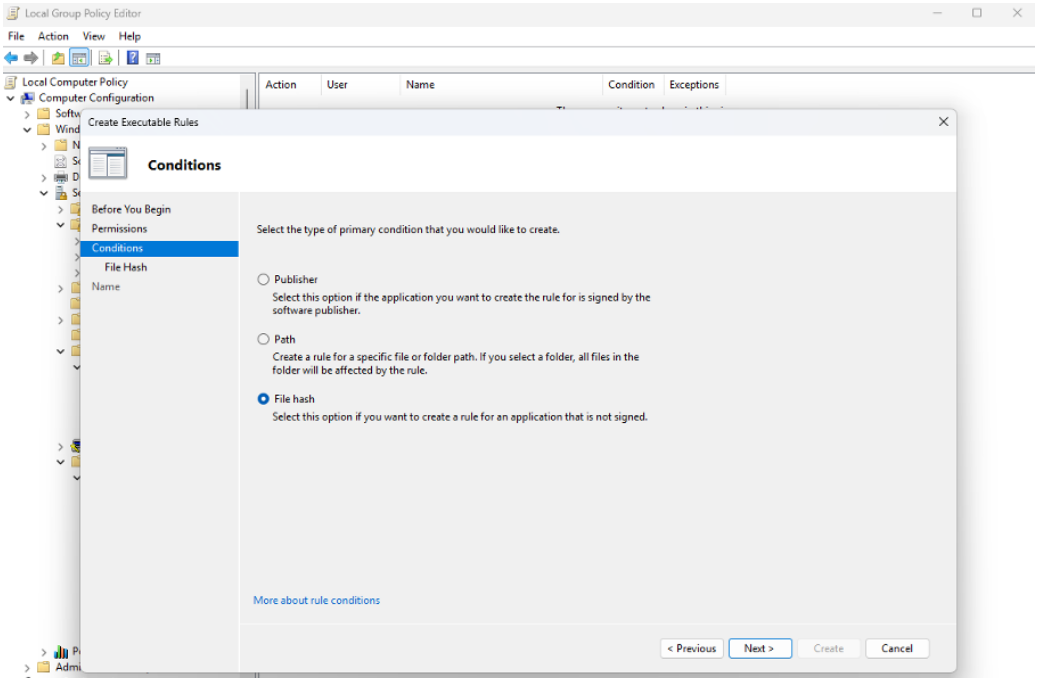
Nastavenie politiky pre aktivovanie application whitelistingu

V rámci skupinových politík v operačných systémoch Windows (GPO) vynútime kontrolu spúšťaných aplikácií a skriptov formou whitelistingu zo zoznamu hashov, ktorý sme vytvorili v predošlom kroku.

Local Security Policy – Application Control Policies – Applocker (resp. Local Computer Policy – Computer Configuration – Windows Settings – Security Settings – Application Control Policies – AppLocker – Executable Rules)

- V AppLocker / Executable Rules nastavíme nové pravidlo, pre ktoré použijeme zoznam hashov
- *nástroj Applocker je dostupný len v edíciách Windows 10 Pro, Windows 11 Pro a vyšších





Testovanie a aplikácia

Otestujte váš nový golden image (resp. obraz systému nakonfigurovaný v jeho konečnej „dokonalej" verzii, ktorý sa používa na nasadzovanie nových inštancií systému na zariadenia zamestnancov), či obsahuje a bezpečne dovoľuje spúšťať všetky aplikácie a skripty, ktoré vaši zamestnanci potrebujú. Komplexnejšie aplikácie nám pri prvom teste nemusia fungovať, pokiaľ sme nezahrnuli do zoznamu všetky spustiteľné komponenty, ktoré aplikácie potrebujú. Odporúča sa preto zaviesť krátke adopčné obdobie, kedy budeme monitorovať hlásenia spúšťaných súborov bez blokovania, aby sme odstránili prípadné nedostatky nášho whitelistu.

Politika povoľovania spúšťania súborov a skriptov na základe zoznamu môže blokovať aj legitímne aplikácie, pokiaľ ich opomenieme pri tvorbe zoznamu. Berte tiež do úvahy, že akýkoľvek inštalovaný program alebo dodatočne nahraný skript budete potrebovať po schválení doplniť do zoznamu hashov.

Publisher rules, alebo ako si uľahčiť administráciu whitelistu

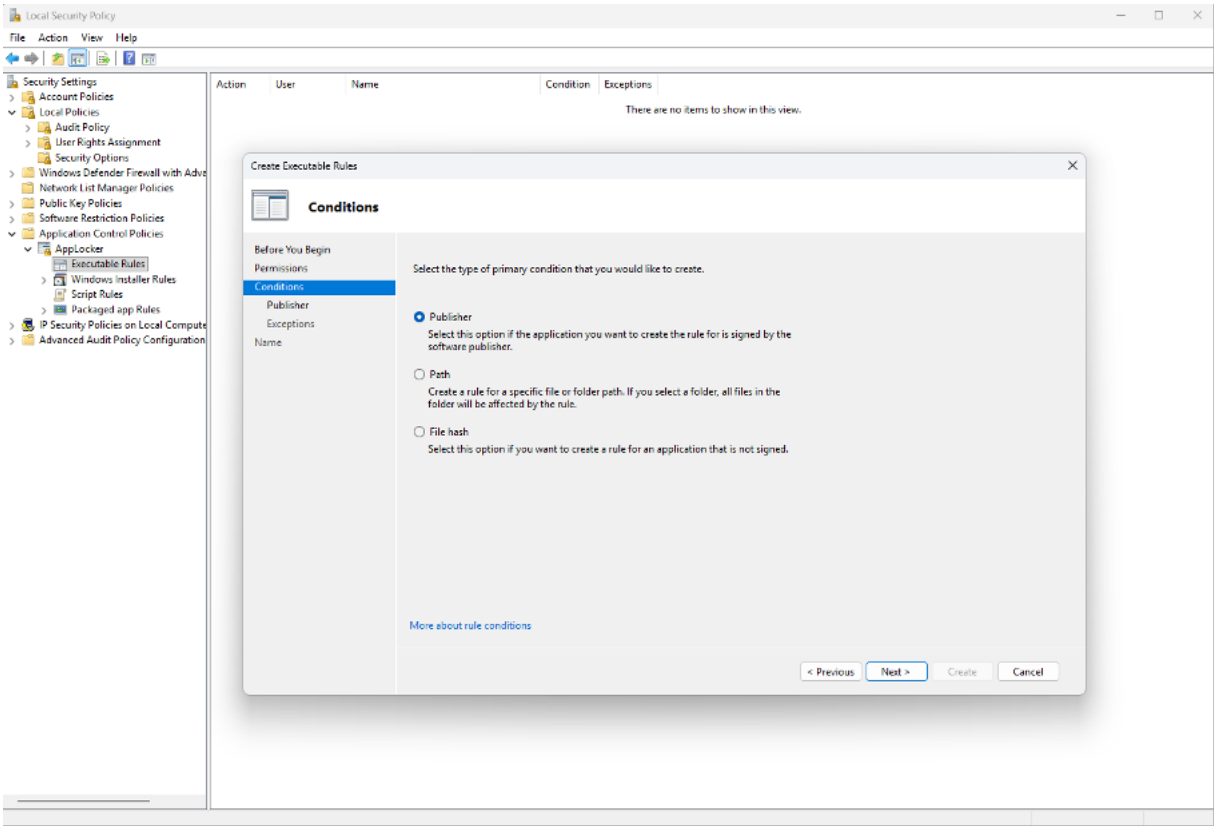
Udržiavanie whitelistu je pomerne náročné, najmä v súvislosti s často aktualizovanými spustiteľnými súbormi, akými sú systémové súbory samotného OS Windows. Prácu si môžeme uľahčiť adaptovaním hybridného prístupu, kedy tieto súbory, resp. systémové zložky vynecháme z whitelistingu a budeme ich chrániť pomocou pravidiel pre kryptograficky podpísané súbory (publisher rules v nástroji AppLocker). Tento prístup síce neposkytuje rovnakú úroveň bezpečnosti, ako kontrola hashov, no v bežných podmienkach ho môžeme pokladať za dostatočnú náhradu.
Systémové súbory vynecháme pri tvorbe whitelistu, keď použijeme nasledujúci príkaz:

```
dir c:\*.exe /a /s /b | findstr /v /i "c:\\windows c:\\program" >> zoznam.txt
```

Tento príkaz odfiltruje (/v) všetky súbory, ktoré sa nachádzajú v systémových zložkách s reťazcami „windows" a „program" v názvoch, bez ohľadu na to, či vo veľkých alebo malých písmenách (/i). Odfiltrujeme teda súbory v zložkách C:\Windows, C:\Program Files a C:\ProgramData.
Zoznam nasadíme vyššie popísaným spôsobom. Potrebujeme však ešte zabezpečiť ochranu vynechaných zložiek. To dosiahneme povolením spúšťania súborov podpísaných dôveryhodnými kryptografickými certifikátmi spoločnosti Microsoft.

Local Security Policy – Application Control Policies – Applocker (resp. Local Computer Policy – Computer Configuration – Windows Settings – Security Settings – Application Control Policies – AppLocker – Executable Rules)

- V AppLocker / Executable Rules nastavíme nové pravidlo, pre ktoré použijeme zoznam hashov



Ďalšie odporúčania pre zvýšenie bezpečnosti

Pre zvýšenie bezpečnosti prenosu a zdieľania súborov v rámci podnikovej siete môžeme nastaviť aj vynucovanie podpisovania na serveri LDAP, SMB. Tieto možnosti nájdeme v *Local Security Policy – Local Policies – Security Options (resp. Local Computer Policy – Computer Configuration – Windows Settings – Security Settings – Local Policies - Security Options)*

- Domain controller: LDAP server signing requirements Enforcement
- Microsoft network client: Digitally sign communications (always)

Pre zníženie zraniteľnosti voči útokom typu SMB relay môžeme ešte zakázať prichádzajúce autentifikačné požiadavky cez NTLM z klientskych staníc

- Network security: Restrict NTLM: Incoming NTLM traffic

Na záver

Prístup application whitelisting je riešenie, ktoré významne zefektívni ochranu našej infraštruktúry pred spustením škodlivého kódu a minimalizuje riziko spôsobené nevedomosťou a nedbanlivosťou používateľov. Je bezplatným rozšírením schopností vášho antimalvérového riešenia a doplnkovou vrstvou ochrany pre riešenia typu EDR/XDR. Jeho nasadenie sa ponúka najmä v infraštruktúrach obsahujúcich unifikované pracovné stanice alebo skupiny staníc, vzhľadom na nízku administratívnu náročnosť.

Zdroje

- https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol-and-applocker-overview
- https://www.techtarget.com/searchsecurity/definition/application-whitelisting
- https://stackoverflow.com/questions/67410109/how-to-get-md5-hash-only-batch-script
- https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/understanding-the-publisher-rule-condition-in-applocker