ESET Anti-Ransomware nastavenie

Viacvrstvové zabezpečenie pred nežiaducim zašifrovaním dát útočníkom

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

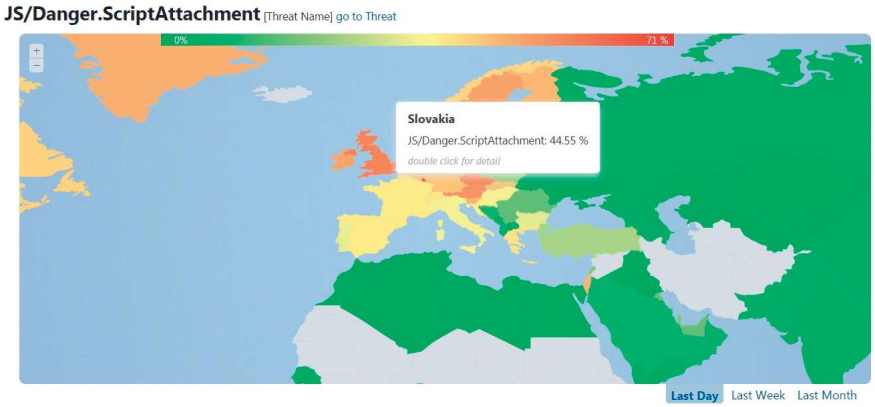
OBSAH

CIEĽ TÝCHTO TECHNICKÝCH INŠTRUKCIÍ

V týchto technických inštrukciách vám opíšeme optimálne nastavenie vašich bezpečnostných riešení spoločnosti ESET tak, aby vás čo najlepšie chránili pred súčasnými formami ransomwaru a taktiež pred najčastejšími spôsobmi infekcie. Cieľom je ešte lepšie chrániť ESET zákazníkov pred prepuknutím infekcie ransomwaru, pri ktorej môže útočník zašifrovať cenné firemné dáta a za ich odšifrovanie požadovať výkupné. Viac informácií o tom, čo je ransomware, nájdete v dokumente *Filecodery – dvojitá prevencia a liečba*.

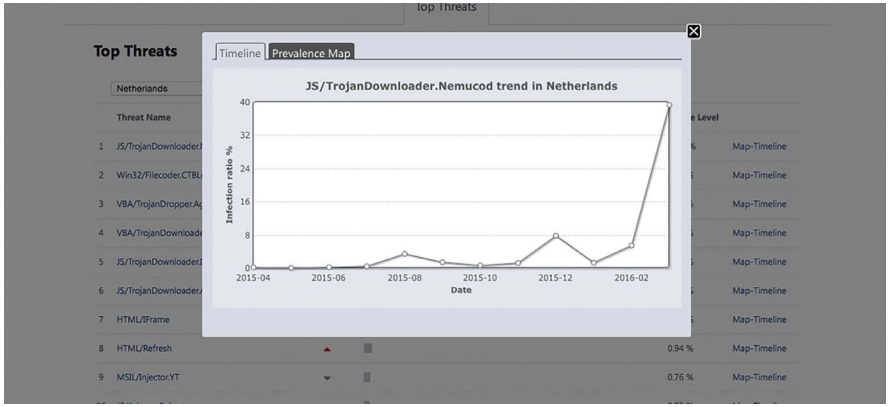
PREČO PRÁVE TIETO DODATOČNÉ NASTAVENIA

V niektorých obdobiach môže takmer polovica všetkého škodlivého kódu, ktorý ESET deteguje na Slovensku, viesť k infekcii ransomwarom.



Súčasné útoky ransomwarom používajú pokročilé techniky pre infikovanie vášho zariadenia. Ľudí presvedčia, aby vo svojom zariadení spustili takzvaný dropper, ktorý do zariadenia stiahne samotný škodlivý kód, ktorý začne proces šifrovania. Pridaním droppera do e-mailovej správy sa útočníci snažia zamedziť tomu, aby bol bezpečnostným riešením detegovaný. Vo väčšine prípadov používajú slušne vyzerajúci phishingový e-mail, ktorý obsahuje zazipovanú prílohu. Tento ZIP súbor väčšinou obsahuje javascriptový súbor typu .JS. Keďže JavaScript používa veľké množstvo webstránok, je nemožné ho blokovať priamo v prehliadači. Okrem toho Windows spúšťa JavaScript okamžite.

Javascriptový kód v dropperi je obfuskovaný a neustále modifikovaný tak, aby sa vyhol detekcii. Toto nám dáva možnosť ovplyvniť spustenie potenciálne škodlivého kódu cez štandardné procesy použitím viacerých bezpečnostných modulov.

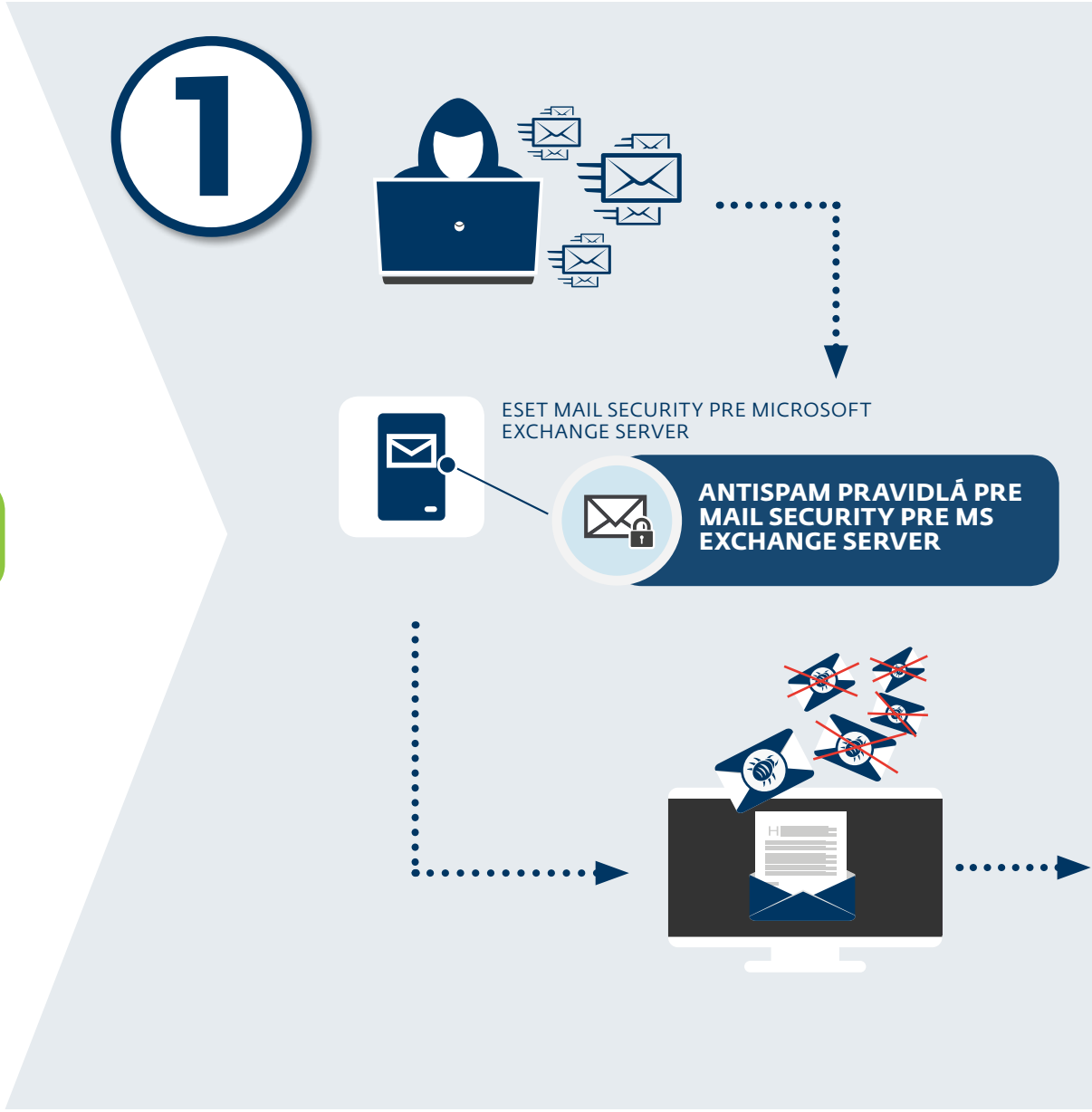


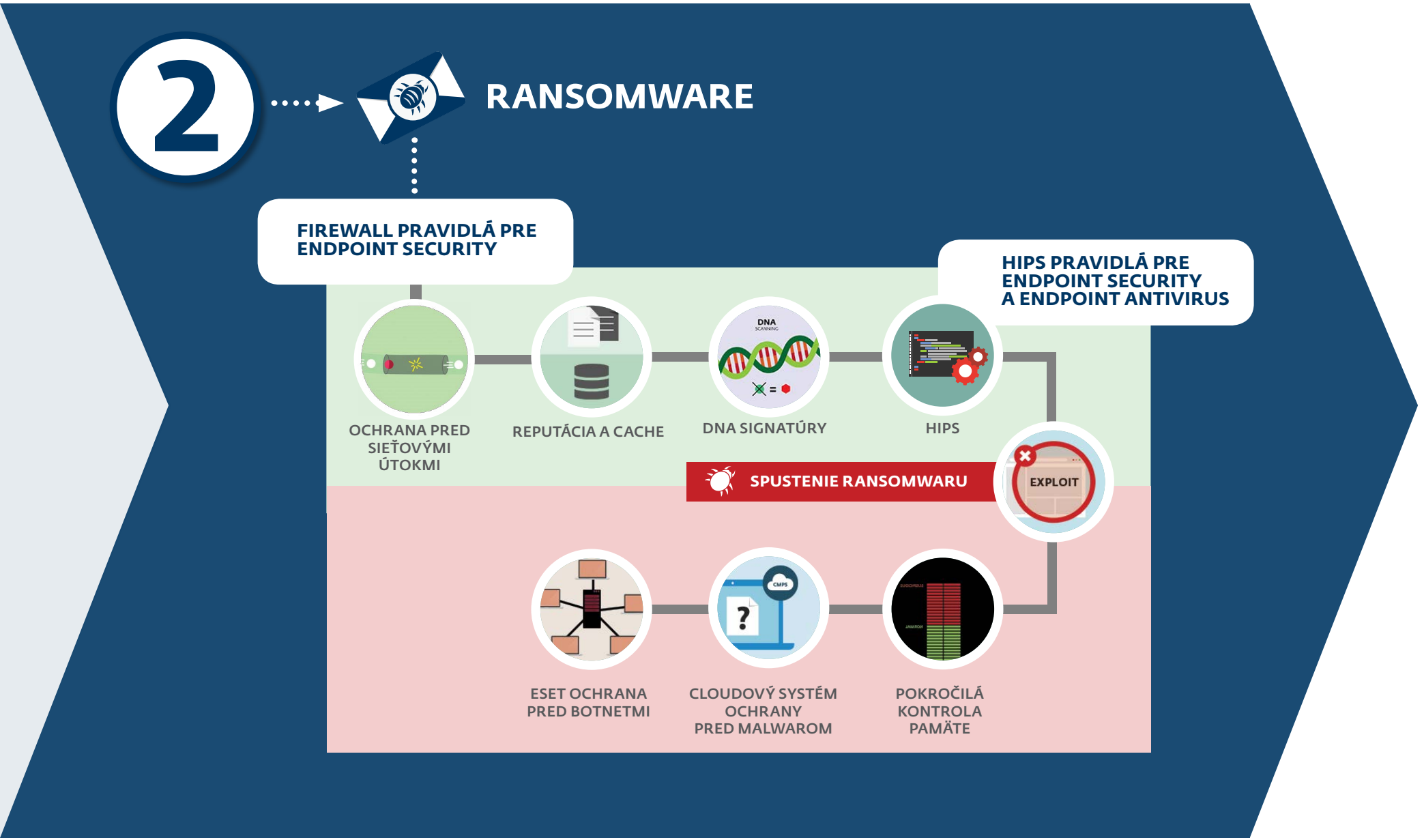
Upozornenie:
ESET Anti-Ransomware nastavenie a politiky sú generické a môžu sa líšiť v jednotlivých podnikových prostrediach. Odporúčame najskôr otestovať nastavenia pre každú implementáciu v testovacom prostredí.

ESET ANTI-RANSOMWARE NASTAVENIA PRE FIRMY

Dodatočné ESET Anti-Ransomware nastavenia dokážu zabrániť stiahnutiu škodlivému kódu tým, že zablokujú spôsob, ktorým ransomware infikuje zariadenia (použitím javascriptového droppera). Keďže tento prístup je veľmi efektívny, rozhodli sme sa dodatočné nastavenia vysvetliť v týchto technických inštrukciách. Taktiež vám ponúkame možnosť stiahnutia týchto nastavení vo forme konfigurácií politík, ktoré môžete do vášho firemného prostredia implementovať použitím nástroja ESET Remote Administrator.

STIAHNUŤ NASTAVENIA



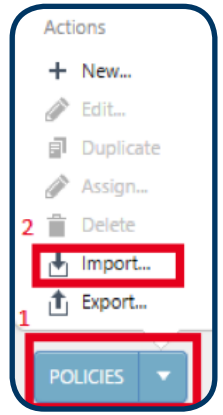

2
RANSOMWARE
FIREWALL PRAVIDLÁ PRE ENDPOINT SECURITY
HIPS PRAVIDLÁ PRE ENDPOINT SECURITY A ENDPOINT ANTIVIRUS
DNA
SCANNING
OCHRANA PRED SIEŤOVÝMI ÚTOKMI
REPUTÁCIA A CACHE
DNA SIGNATÚRY
HIPS
SPUSTENIE RANSOMWARU
EXPLOIT
CMPS
ESET OCHRANA PRED BOTNETMI
CLOUDOVÝ SYSTÉM OCHRANY PRED MALWAROM
POKROČILÁ KONTROLA PAMÄTE

ANTISPAM PRAVIDLÁ PRE ESET MAIL SECURITY PRE MS EXCHANGE

Použitím správnych antispam pravidiel sú príchodzie e-maily filtrované už na samotnom mail serveri. Zabezpečí to, že príloha obsahujúca škodlivý dropper nebude doručená do schránky koncového používateľa a ransomware nedostane šancu spustiť sa.

Ako importovať a aplikovať politiky*

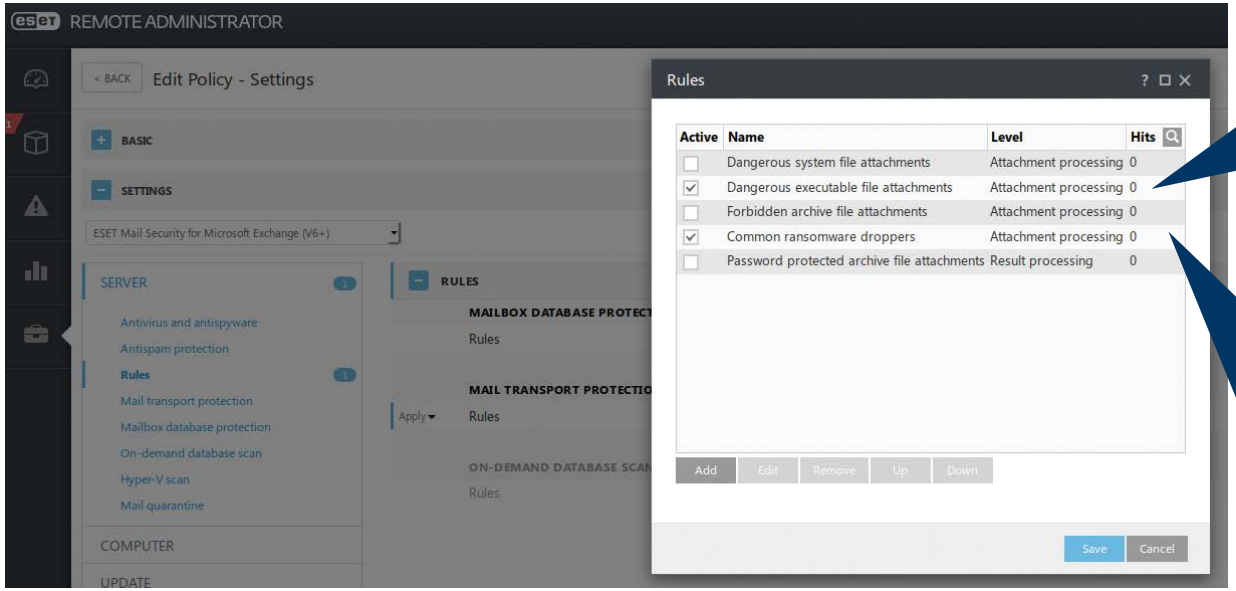
1. Prihláste sa do ERA 6 webkonzoly
2. Nájdite SPRÁVCA > Politiky (ADMIN > Policies)
3. Potom si vyberte "Politiky" (Policies) a následne "Import"
4. Importujte politiky jednu po druhej
5. Upravte politiky *skupine* alebo *klientovi*

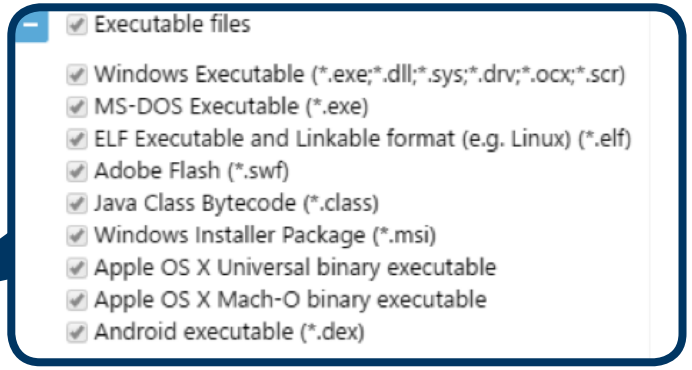


*** Opakovanie pri ostatných nastaveniach nie je nutné.**

Dôležité:

Upgradnite ESET Mail Security pre Microsoft Exchange Server na aktuálne najnovší build 6.3.x alebo vyšší, aby ste boli istý, že pravidlá filtrovania naozaj fungujú.





Bežné ransomware droppery, ktoré blokujú nasledovné prípony*:

*.js
*.hta
*.docm
*.xlsm
*.pptm
*.vbs
*.bat

* V prípade súborov **Microsoft Office budú zablokované aj súbory s makrami (docm, xlsm a pptm)**. Ak sa vo vašej firme takéto súbory používajú, toto pravidlo musí byť prestavené alebo vypnuté.

FIREWALL PRAVIDLÁ PRE ENDPOINT SECURITY

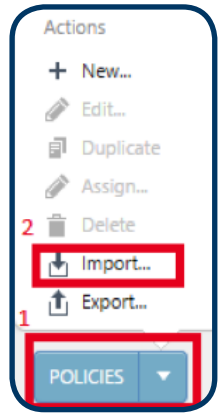
Ak sa dropper so škodlivým kódom spustí, je vysoká pravdepodobnosť, že web ochrana zablokuje stiahnutie samotného malwaru. V prípade, že sa škodlivý súbor nezablokuje pri sťahovaní a spustí sa, ESET Endpoint Security dokáže zabrániť v ďalšej komunikácii s útočníkovými tzv. C&C servermi vďaka modulu sieťovej ochrany, ktorý je súčasťou integrovaného firewallu.

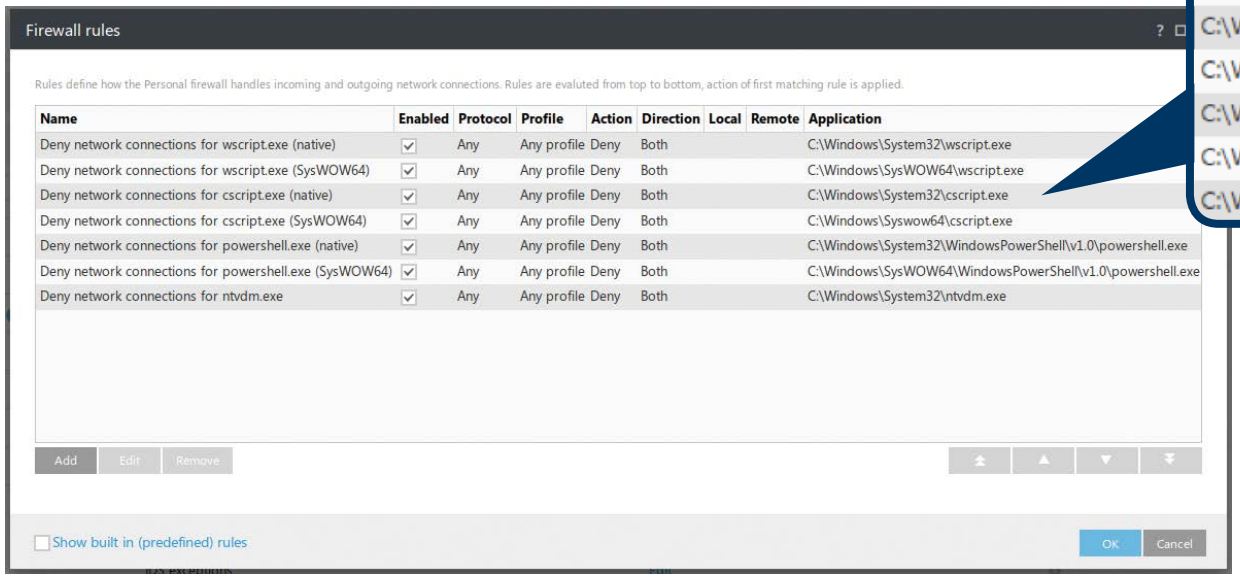
Použitím týchto firewall pravidiel dokáže ESET Endpoint Security zablokovať sťahovanie malwaru a zakázať iným skriptom prístup k internetu.

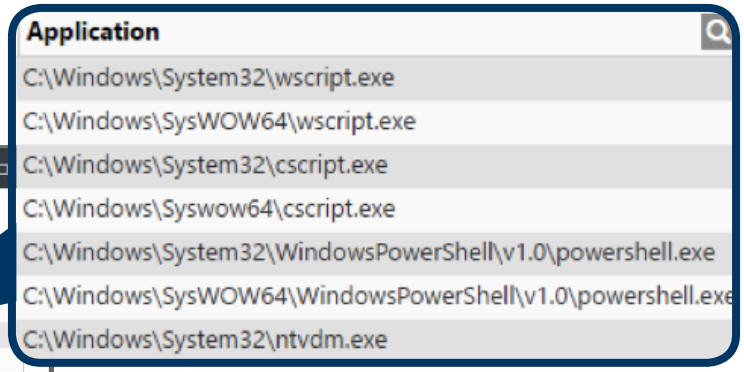
Ako importovať a aplikovať politiky

1. Prihláste sa do ERA 6 webkonzoly
2. Nájdite ADMIN > Policies
3. Potom si vyberte „Policies" a následne „Import"
4. Importujte politiky jednu po druhej
5. Upravte politiky *skupine* alebo *klientovi*

Prosím dbajte na to, že importovaním firewall nastavení budú existujúce firewallové pravidlá prepísané.







DÔLEŽITÉ

- Táto politika funguje len v kombinácii s ESET Endpoint Security práve vďaka integrovanému firewall modulu.
- Pri týchto pravidlách platí, že aj legitímne aplikácie môžu používať tieto spustiteľné súbory. Pred plnou implementáciou do vášho systému vám preto odporúčame ich najskôr otestovať.

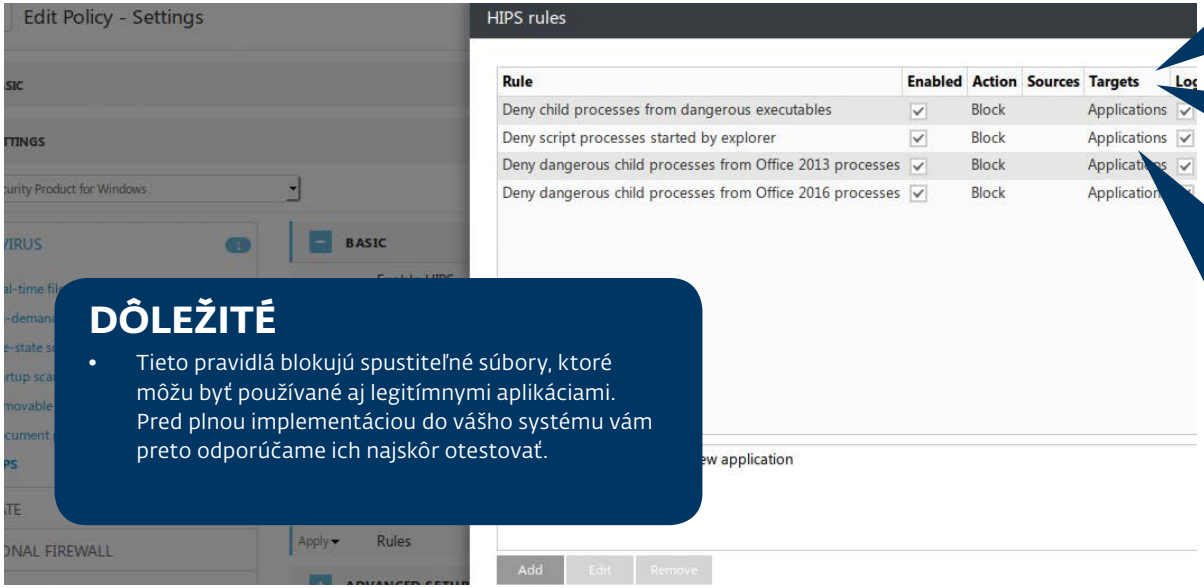
HIPS PRAVIDLÁ PRE ENDPOINT SECURITY A ENDPOINT ANTIVIRUS

Host-based Intrusion Prevention System (HIPS) monitoruje systém a dokáže zablokovať akcie procesov predtým, než sa vykonajú. Zakázaním štandardného spustenia JavaScriptu a iných skriptov sa zabráni ich vykonaniu a tým aj následnému stiahnutiu ransomwaru.

HIPS je taktiež súčasťou ESET File Security pre Windows Server, vďaka čomu je aplikovateľný aj na serveroch. Prosím, dbajte na to, že HIPS nebude vidieť rozdiel pri legitímnych skriptoch, ktoré sa spustia v produkčnom prostredí.

Ako importovať a aplikovať politiky

1. Prihláste sa do ERA 6 webkonzoly
2. Nájdite ADMIN > Policies
3. Potom si vyberte „Policies" a následne „Import"
4. Importujte politiky jednu po druhej
5. Upravte politiky *skupine* alebo *klientovi*



Blokuje procesy nebezpečných aplikácií

Application
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\Syswow64\cscript.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\ntvdm.exe

Blokuje procesy skriptov spúšťaných explorerom

C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe

Blokuje nebezpečné procesy Microsoft Office 201x

C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\ntvdm.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

DÔLEŽITÉ

- Tieto pravidlá blokujú spustiteľné súbory, ktoré môžu byť používané aj legitímnymi aplikáciami. Pred plnou implementáciou do vášho systému vám preto odporúčame ich najskôr otestovať.

VÝSLEDKY TESTU ESET ANTI-RANSOMWARE NASTAVENIA

S kompletným ESET Anti-Ransomware nastavením od mail serverov cez endpointy až po servery sú ransomware e-maily s droppermi v prílohách odfiltrované ešte predtým, než sú detegované ako škodlivý kód alebo ransomware. S týmito zosilnenými nastaveniami sme na endpointoch vykonali niekoľko testov, pri ktorých sme vypli všetky detekčné vrstvy bezpečnostných riešení ESETu. Testy ukázali, že pri použití nastavení nemá skriptový ransomware šancu zašifrovať systém a sieť.

ESET Anti-Ransomware nastavenie je preto zosilnením bezpečnostných riešení ESETu. Minimalizuje šancu infekcie ransomwarom a predchádza zašifrovaniu cenných firemných dát.