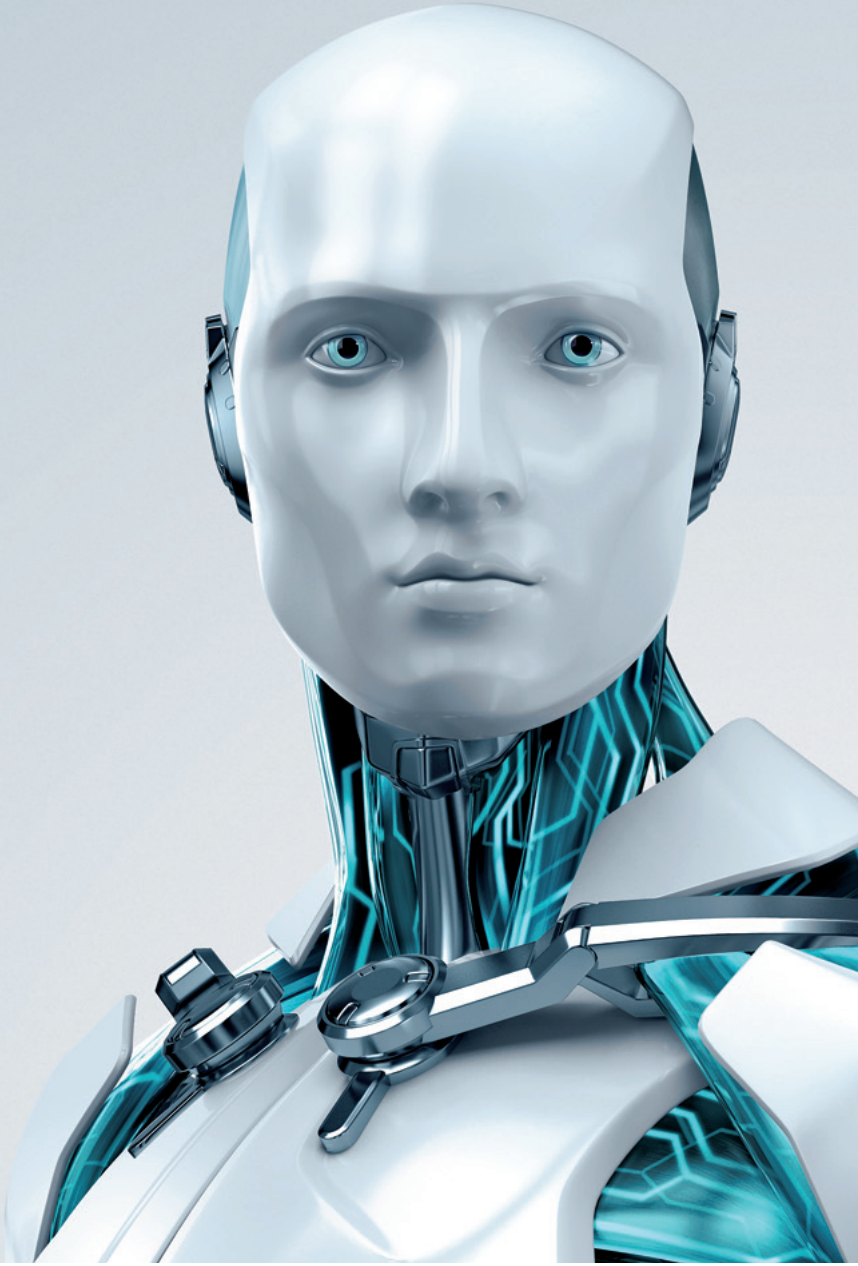
OCHRONA PRZED RANSOMWARE

Konfiguracja ustawień

Wprowadzanie zmian i proponowanych w niniejszym dokumencie polityk bezpieczeństwa polecamy wyłącznie administratorom, posiadającym szczegółową wiedzę nt. swojej sieci firmowej oraz realizowanych w niej polityk bezpieczeństwa. Wskazane ustawienia dotyczą programów ESET dla firm w wersji 6.x lub wyższej.

Rekomendujemy, by sprawdzić zawartość proponowanych polityk bezpieczeństwa zanim zaimplementujesz je w swoim środowisku sieciowym. Nierozważne ich zastosowanie może doprowadzić do wstrzymania pracy lub uszkodzenia środowiska produkcyjnego. Jeżeli wprowadzona polityka spowoduje konflikt w Twojej sieci firmowej, zawsze możesz ją cofnąć.



SPIS TREŚCI:

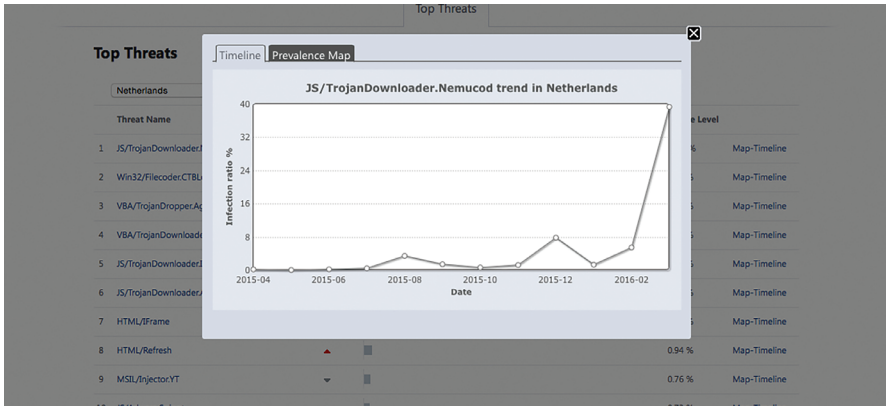
WSTĘP

W niniejszym artykule wskażemy najbardziej optymalne ustawienia dla produktów ESET oraz najpowszechniejsze scenariusze rozprzestrzeniania się infekcji w postaci szkodliwego oprogramowania ransomware. Celem firmy ESET jest zapewnienie użytkownikom jeszcze skuteczniejszej ochrony przed zagrożeniami ransomware, szyfrującymi dane i żądającymi okupu za ich odblokowanie.

DLACZEGO WARTO KORZYSTAĆ Z DODATKOWYCH USTAWIEŃ?

Obecnie ataki ransomware przebiegają z wykorzystaniem socjotechniki oraz wiadomości phishingowych, które próbują przekonać użytkownika, że pochodzą od znanego nadawcy. Cyberprzestępcy przekonują użytkownika, by ten sam uruchomił tzw. dropper, dołączony do wiadomości e-mail. Użytkownik po otwarciu załącznika uaktywnia złośliwy kod. Ten pobiera złośliwe oprogramowanie i rozpoczyna proces szyfrowania. W ten sposób twórcy programów typu ransomware próbują uniknąć wykrycia przez aplikacje antywirusowe i systemy firewallowe.

W większości przypadków wspomniana wiadomość zawiera załącznik w postaci pliku ZIP. Archiwum to zawiera w sobie z kolei plik JavaScript, a ponieważ JavaScript jest wykorzystywany przez wiele stron internetowych, niemożliwe jest zablokowanie go w przeglądarce. Dodatkowo sam system Windows także korzysta z JavaScript. Właśnie dlatego cyberprzestępcy wykorzystują tę możliwość do umieszczenia nowych wersji ransomware w plikach JavaScript.

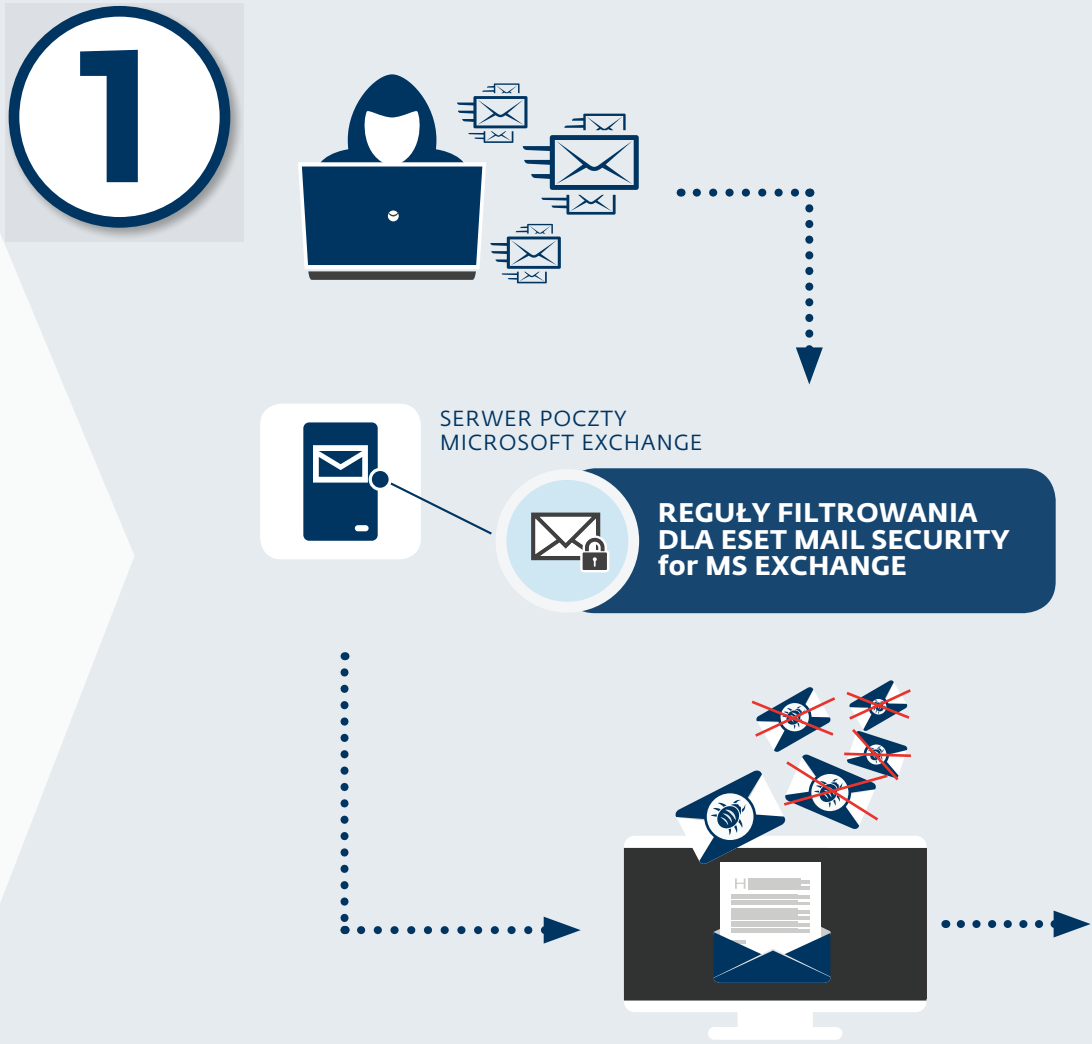


Ustawienia i polityki chroniące przed ransomware są określane rodzajowo i mogą być różne w zależności od środowiska. Rekomendujemy, by sprawdzić konfigurację zanim w pełni zaimplementujesz polityki w swoim środowisku.

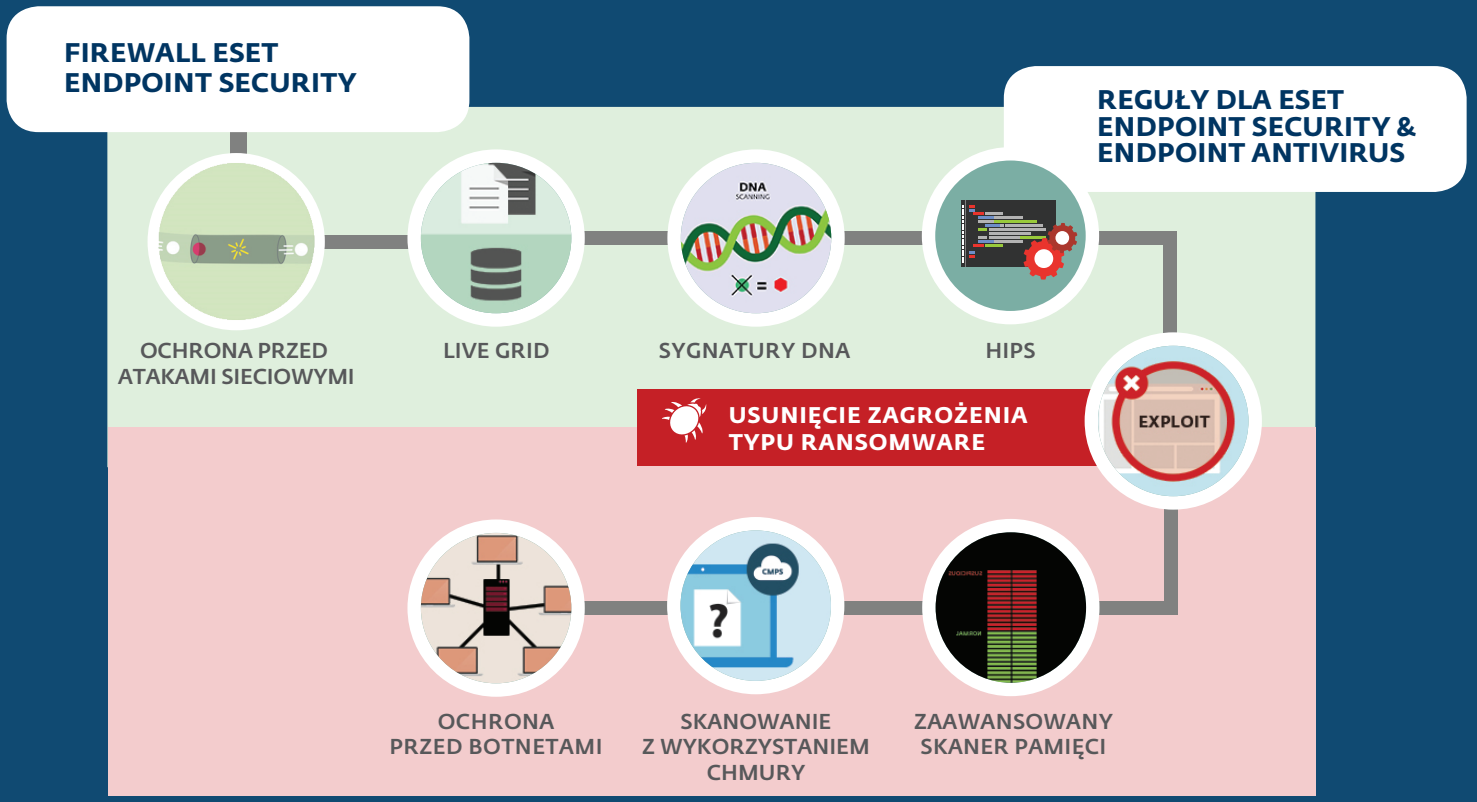
KONFIGURACJA USTAWIEŃ PROGRAMÓW ESET DLA BIZNESU

Chcąc zapobiec pobraniu złośliwego oprogramowania (np. z użyciem dropper'a JavaScript) skonfiguruj swoje dodatkowe ustawienia.

Taką konfigurację jesteś w stanie wdrożyć za pomocą naszego ESET Remote Administrator. Poniżej szczegółowo opisujemy jak to zrobić.



2 RANSOMWARE



USTAWIENIE REGUŁ ANTYSPAMOWYCH ESET MAIL SECURITY FOR MS EXCHANGE SERWER ORAZ REGUŁ HIPS DLA ESET FILE SECURITY

Stosując odpowiednie reguły antyspamowe zainfekowane wiadomości są odrzucane już na etapie ochrony serwerów poczty przez co nie zostają dostarczone do skrzynki pocztowej finalnego użytkownika. Dzięki temu, złośliwe oprogramowanie nie ma możliwości aktywowania się. Moduł HIPS jest częścią ESET File Security dla Windows Server dzięki czemu opcja ta ma również zastosowanie do serwerów plików. Pamiętaj, ze system HIPS nie będzie wpływał negatywnie na działanie prawidłowych skryptów uruchamianych z lokalizacji systemowych.

POBIERZ POLITYKI

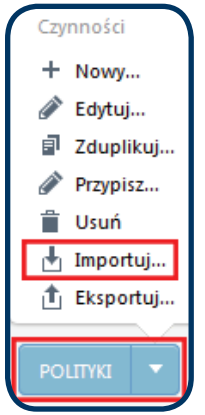
Przed wysłaniem polityk należy bezwzględnie zaznajomić się z ich zawartością. Nierozważne ich zastosowanie może doprowadzić do wstrzymania pracy lub uszkodzenia środowiska produkcyjnego.

Uwaga:

Zaktualizuj ESET Mail Security dla Microsoft Exchange Server do wersji 6.3 lub nowszej, by zapewnić reguły filtrowania działały prawidłowo.

Jak importować i aktywować polityki*

1. Zaloguj się do konsoli webowej (ESET Remote Administrator 6)
2. Przejdź do ADMINISTRATOR -> Polityki
3. Kliknij przycisk Polityki i następnie Importuj...
4. Zaimportuj polityki pojedynczo
5. Przypisz polityki do odpowiednich grup

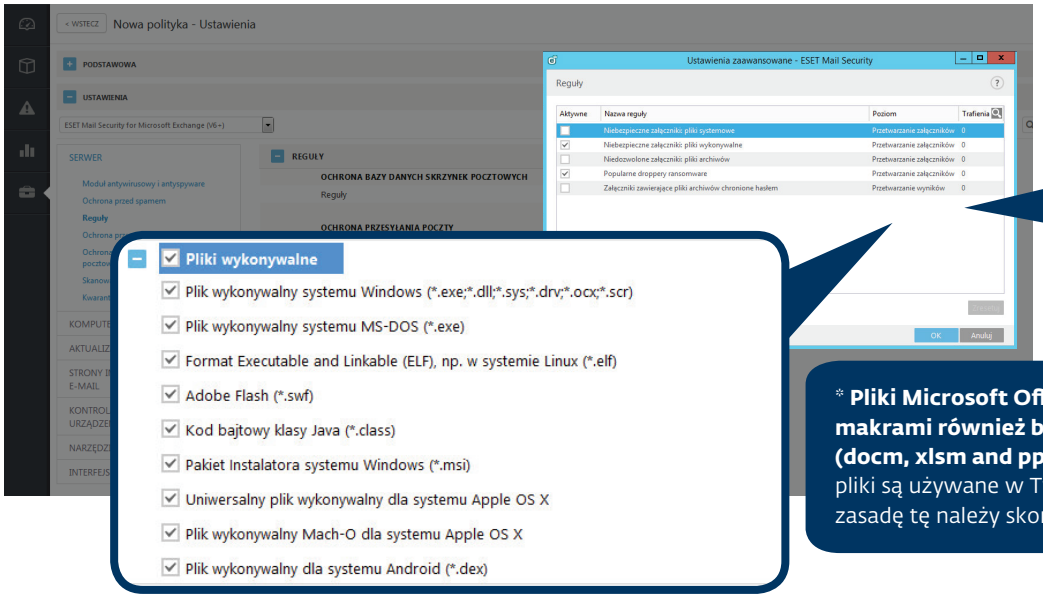


*** Jeśli polityka wykonywanych plików jest już zdefiniowana nie trzeba jej konfigurować.**

Jeżeli wprowadzona polityka spowoduje konflikt w Twojej sieci firmowej pamiętaj, że możesz ją cofnąć.

Cofnięcie przypisania polityki:

W panelu "Administrator" w sekcji "polityki" po wybraniu konkretnej polityki należy wybrać po prawej stronie: "Klienty" lub "Grupy". Po wybraniu odpowiednich obiektów należy wybrać "Cofanie przypisywania"



Lista rozszerzeń blokowanych dropperów*:

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

*** Pliki Microsoft Office z włączonymi makrami również będą blokowane (docm, xlsm and pptm).** Jeżeli takie pliki są używane w Twojej polityce, zasadę tę należy skorygować lub wyłączyć.

USTAWIENIA FIREWALLA DLA ESET ENDPOINT SECURITY

Pomimo uruchomienia złośliwego kodu przez dropper'a, aplikacja ESET Endpoint Security dalej będzie zapobiegać pobraniu złośliwego oprogramowania. A wszystko to dzięki zintegrowanemu firewall'owi. Po zastosowaniu tych reguł ESET Endpoint Security będzie blokować pobieranie infekcji oraz połączenia innych skryptów do Internetu.

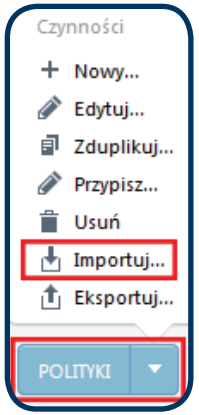
POBIERZ POLITYKI

Przed wysłaniem polityk należy bezwzględnie zaznajomić się z ich zawartością. Nierozważne ich zastosowanie może doprowadzić do wstrzymania pracy lub uszkodzenia środowiska produkcyjnego.

Jak importować i aktywować polityki

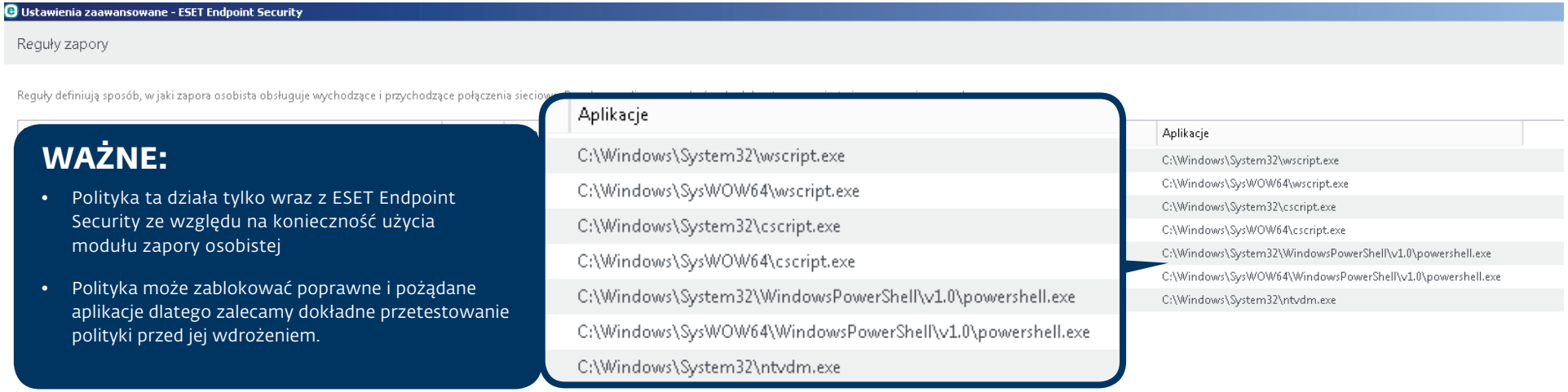
1. Zaloguj się do konsoli webowej (ESET Remote Administrator 6)
2. Przejdź do ADMINISTRATOR -> Polityki
3. Kliknij przycisk Polityki i następnie Importuj...
4. Zaimportuj polityki pojedynczo
5. Przypisz polityki do odpowiednich grup

Import reguł Firewall może spowodować zastąpienie reguł już istniejących.



Jeżeli wprowadzona polityka spowoduje konflikt w Twojej sieci firmowej pamiętaj, że możesz ją cofnąć.

Cofnięcie przypisania polityki:
W panelu "Administrator" w sekcji "polityki" po wybraniu konkretnej polityki należy wybrać po prawej stronie: "Klienty" lub "Grupy". Po wybraniu odpowiednich obiektów należy wybrać "Cofanie przypisywania"



WAŻNE:

- Polityka ta działa tylko wraz z ESET Endpoint Security ze względu na konieczność użycia modułu zapory osobistej
- Polityka może zablokować poprawne i pożądane aplikacje dlatego zalecamy dokładne przetestowanie polityki przed jej wdrożeniem.

USTAWIENIA SYSTEMU HIPS DLA ESET ENDPOINT SECURITY & ESET ENDPOINT ANTIVIRUS

HIPS (System zapobiegania włamaniom działający na hoście) chroni system od wewnątrz monitorując aktywności systemu operacyjnego. Dzięki temu jest w stanie przerwać nieautoryzowane działania procesów, zanim te zaczną być w pełni wykonywane. Blokując wykonywanie skryptów - JavaScript i innych, ransomware nie może pobrać złośliwego oprogramowania.

POBIERZ POLITYKI

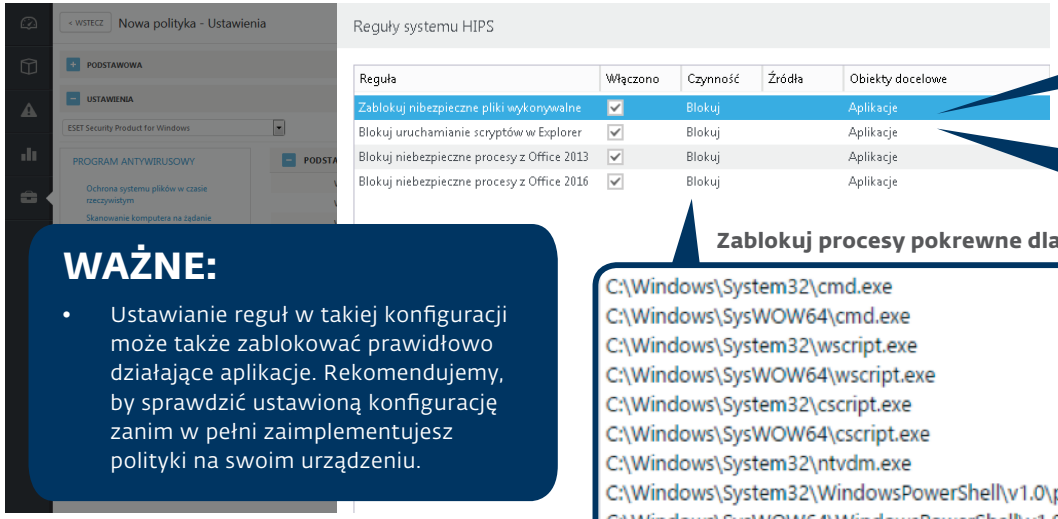
Przed wysłaniem polityk należy bezwzględnie zaznajomić się z ich zawartością. Nierozważne ich zastosowanie może doprowadzić do wstrzymania pracy lub uszkodzenia środowiska produkcyjnego.

Jak importować i aktywować polityki

1. Zaloguj się do konsoli webowej (ESET Remote Administrator 6)
2. Przejdź do ADMINISTRATOR -> Polityki
3. Kliknij przycisk Polityki i następnie Importuj...
4. Zaimportuj polityki pojedynczo
5. Przypisz polityki do odpowiednich grup

Jeżeli wprowadzona polityka spowoduje konflikt w Twojej sieci firmowej pamiętaj, że możesz ją cofnąć.

Cofnięcie przypisania polityki:
W panelu "Administrator" w sekcji "polityki" po wybraniu konkretnej polityki należy wybrać po prawej stronie: "Klienty" lub "Grupy". Po wybraniu odpowiednich obiektów należy wybrać "Cofanie przypisywania"



Zablokuj skrypty

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

Zablokuj procesy pokrewne

Aplikacje
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

Zablokuj procesy pokrewne dla 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

WAŻNE:

- Ustawianie reguł w takiej konfiguracji może także zablokować prawidłowo działające aplikacje. Rekomendujemy, by sprawdzić ustawioną konfigurację zanim w pełni zaimplementujesz polityki na swoim urządzeniu.

TEST SKUTECZNOŚCI USTAWIEŃ OCHRONY PRZED RANSOMWARE

Zastosowanie wszystkich wskazanych ustawień w programach ESET - od serwera pocztowego, aż po stację kliencką - sprawia, że wiadomości e-mail zawierające droppery są przechwytywane i blokowane zanim jeszcze zostaną zidentyfikowane jako złośliwy ransomware. Przeprowadzone testy dowiodły, że stacje klienckie z tak wzmocnionymi ustawieniami ochrony, nawet przy wyłączonych zabezpieczeniach programów ESET są odporne na infekcje zagrożeń szyfrujących.

Wskazane w niniejszym dokumencie ustawienia ochrony dla rozwiązań ESET minimalizują ryzyko infekcji komputerów przez złośliwe oprogramowanie typu ransomware i ryzyko zaszyfrowania kluczowych firmowych danych.