

McAfee Enterecept Desktop Edition

Ochrona komputerów biurkowych przed włamaniami

Produktywność każdego uczestnika procesu gospodarczego zależy od tego, czy może on łatwo połączyć się z siecią. Im więcej użytkowników korzysta z sieci i im więcej ważnych danych jest przechowywanych na komputerach osobistych, tym bardziej skomplikowane staje się zapewnienie bezpieczeństwa. Obecnie komputery osobiste niemal dorównują pod względem mocy serwerom o znaczeniu krytycznym. Skutki działania niszczycielskich robaków, takich jak Slammer, Lovsan czy Nachi, wskazują na to, że trzeba chronić je skuteczniej, niż może to zapewnić technologia antywirusowa.

Jak informuje CERT (Computer Emergency Response Team), liczba zgłaszanych prób złamania zabezpieczeń podwaja się z każdym rokiem. Wraz z pojawianiem się nowych technik ataku coraz trudniej jest powstrzymać napastników. Do działania na coraz większej liczbie platform, w tym często na systemach operacyjnych komputerów biurkowych, skłania ich niekiedy ujawnienie luk w zabezpieczeniach. Szkodliwe programy dzięki różnym wyrafinowanym metodom przedostają się przez tradycyjne zapory i zabezpieczenia graniczne, które nie są już w stanie skutecznie chronić komputerów osobistych. Duże pole do popisu daje napastnikom również to, że komputery osobiste są często bezpośrednio podłączone do Internetu.

Zainstalowanie na czas każdej poprawki zabezpieczeń jest w praktyce niemożliwe, nawet jeśli takie działanie jest uznawane za priorytetowe. Znane już luki w zabezpieczeniach stają się celem dla hakerów, którzy atakują komputery biurkowe i aplikacje, wykorzystując robaki i przepełnienia buforu. Administratorzy systemów i specjaliści od zabezpieczeń mają do czynienia z następującymi zjawiskami:

- szybko zwiększająca się liczba luk w zabezpieczeniach
- coraz bardziej wyrafinowane techniki ataku
- nieużyteczność starszych zabezpieczeń wobec obecnych zagrożeń.

Rozwiązanie McAfee Enterecept

McAfee® Enterecept® Desktop Edition stanowi uzupełnienie do wielokrotnie nagradzanych rozwiązań McAfee do ochrony serwerów. Produkt ten skutecznie chroni przedsiębiorstwa przed atakami wykorzystującymi techniki zarówno znane, jak i jeszcze nierozpoznane. Opatentowana technologia chroni komputery biurkowe przed znanymi i nieznanymi rodzajami ataku. Blokując te ataki, McAfee Enterecept znacznie ogranicza przestoje, zmniejsza koszty związane z bezpieczeństwem i chroni dane o znaczeniu krytycznym. McAfee Enterecept zapobiegawczo chroni komputery biurkowe, ponieważ analizuje żądania, które są zgłaszane do systemu operacyjnego, przed ich przetworzeniem. W odróżnieniu od innych zabezpieczeń McAfee Enterecept opiera się na kombinacji sygnatur i modeli zachowania, aby zapobiec zarówno znanym, jak i nieznanym atakom, a nie tylko wykrywać je i informować o ich wystąpieniu. McAfee Enterecept to uznany lider oprogramowania chroniącego przed włamaniami.

Korzyści, jakie daje McAfee Enterecept

- Mniej przestołów
 - zapobiega atakom, a nie tylko je wykrywa
 - chroni przed wykorzystywaniem przepełnienia buforu.
- Mniejsze koszty związane z bezpieczeństwem
 - znacznie ogranicza koszty wynikające z przestołów
 - zmniejsza zapotrzebowanie na wyspecjalizowany personel.
- Ochrona majątku
 - chroni dane przechowywane na komputerach osobistych
 - osłania aplikacje
 - chroni reputację firmy.
- Łatwiejsze egzekwowanie COE (środowiska operacyjnego przedsiębiorstwa).

Jak działa McAfee Enterecept Desktop Edition

Program McAfee Enterecept Desktop Edition chroni komputery osobiste przy wykorzystaniu różnych technologii. Rozproszona architektura umożliwia zainstalowanie agenta McAfee Enterecept Agent na każdym komputerze biurkowym w przedsiębiorstwie. Agenty McAfee Enterecept Agent przechwytyją wywołania wysyłane do systemu operacyjnego przez interfejs API i system, a następnie blokują te, które mogą być szkodliwe. McAfee Enterecept określa m.in. proces źródłowy wywołania, użytkownika, który wysłał wywołanie, zasoby, na których operuje wywołanie, oraz uprawnienia użytkownika związane z wywołaniem. Na podstawie tych informacji wywołania są porównywane z odpowiednimi modelami zachowania i sygnaturami znanych ataków.

Następnie McAfee Enterecept blokuje wywołania próbujące wyrządzić jakiegokolwiek szkody lub odpowiadające określonej sygnaturze ataku. Wszystkie działania zapobiegawcze są rejestrowane w systemie zarządzania McAfee Enterecept, co umożliwia ich przeglądanie i tworzenie raportów.

W dołączonej do produktu bazie danych zasad znajduje się w pełni skonfigurowany szablon domyślny z funkcjami dostosowywania, co pozwala na niemal całkowite wyeliminowanie fałszywych trafień. Domyślne zasady zapewniają ponadto szybkie wdrażanie. Zainstalowane na każdym komputerze biurkowym agenty są kontrolowane i aktualizowane przez McAfee Enterecept Management System. Agenty są samowystarczalnymi jednostkami ochronnymi i ich funkcjonowanie nie jest uzależnione od systemu zarządzania. Sprzyja to zarówno niezawodności, jak i większemu bezpieczeństwu.

Agenty pobierają aktualizacje, w tym aktualizacje kodu i nowe definicje ataków, z systemu zarządzania. Cała komunikacja odbywa się za pośrednictwem szyfrowania RC4 i protokołu wymiany kluczy Diffie-Hellman.

McAfee Enterccept Desktop Edition

Ochrona komputerów biurkowych przed włamaniami

Zapobieganie znanym atakom — Dzięki wykorzystaniu obszernej bazy danych rozpoznanych technik ataków program McAfee Enterccept może blokować znane zagrożenia i zapobiegać uszkodzeniu komputerów i serwerów. Do bazy danych wciąż są dopisywane nowe ataki, dzięki czemu McAfee Enterccept identyfikuje je według nazwy.

Zapobieganie nieznanym atakom — McAfee Enterccept wykrywa nierozpoznane ataki za pomocą skutecznej technologii modeli zachowania i zapobiega im. Technologia ta wymusza odpowiednie zachowanie aplikacji i systemu operacyjnego, i blokuje nowe ataki właśnie dlatego, że odbiegają one od z góry zdefiniowanych właściwych modeli zachowania. Połączenie ochrony przez modele zachowania z zapobieganiem konkretnym atakom (na podstawie sygnatury) sprawia, że McAfee Enterccept skutecznie chroni zarówno przed znanymi, jak i nieznanymi zagrożeniami.

Zapobieganie wykorzystaniu przepełnienia buforu — McAfee Enterccept zawiera opatentowaną technologię chroniącą przed wykonaniem kodu wskutek przepełnienia buforu. Na przepełnienia buforu przypada ponad 60% porad CERT i stanowią one największe źródło luk w zabezpieczeniach serwerów. McAfee Enterccept chroni komputery biurkowe przed tymi niebezpiecznymi atakami.

Ochrona zasobów — McAfee Enterccept blokuje zasoby systemowe o znaczeniu krytycznym (pliki, ustawienia, klucze

rejestr, usługi itp.), chroniąc system przed zagrożeniami.

Ochrona przed podniesieniem uprawnień — Wielu napastników dostaje się do konta pozbawionego uprawnień, a następnie stosuje różne techniki w celu uzyskania jak największych praw dostępu. McAfee Enterprise blokuje takie działania i pilnuje, aby napastnicy nie podnosili swojego poziomu uprawnień.

McAfee Enterccept oferuje pięć fabrycznie zdefiniowanych poziomów zasad zabezpieczeń, które umożliwiają administratorom intuicyjne i systematyczne podnoszenie poziomu bezpieczeństwa, od trybu ostrzegania do trybu ochrony. Każdy tryb zapewnia wyższy poziom bezpieczeństwa niż poprzedni. Klienci najpierw używają produktu McAfee Enterccept w trybie ostrzegania, a następnie przechodzą coraz wyżej, aż do trybu ochrony, stopniowo dostrajając swoją instalację McAfee Enterccept i zaostrzając kryteria bezpieczeństwa.

Właściwości

- blokowanie ataków, zanim wyrządzą one jakieś szkody
- bezpieczne, samowystarczalne agenty
- fabrycznie skonfigurowany szablon zasad ze wszystkimi opcjami dostosowywania
- zapobieganie szkodliwemu dostępowi do zasobów systemu
- uzupełnienie dotychczasowej infrastruktury zabezpieczeń.

Wymagania instalacyjne

Agent — Windows®

- Windows 2000 i 2000 Professional Workstation
- Windows NT 4.1 Workstation z dodatkiem SP5 lub nowszym

Informacje o McAfee Security

McAfee Security to seria produktów Network Associates® chroniących firmy przed łamaniem zasad bezpieczeństwa, wirusami i zagrożeniami hybrydowymi. McAfee Security kompleksowo chroni sieć za pomocą najlepszych na rynku technologii antywirusowych, szyfrowania, zapór komputerów biurkowych, wykrywania włamań, oceny podatności i outsourcingu zabezpieczeń. Wszystkie produkty i usługi McAfee Security opierają się na dorobku czołowego światowego ośrodka badającego wirusy AVERT™ (Anti-Virus Emergency Response Team), na którego koncie znajdują się szczepionki przeciwko takim wielkim epidemiom jak LoveLetter, CodeRed i Nimda. Więcej informacji na temat McAfee Security można uzyskać telefonicznie, pod numerem 888-VIRUS-NO, oraz w Internecie na stronie

<http://www.mcafeesecurity.com>.

Wszystkie produkty Network Associates® są obsługiwane przez program PrimeSupport® i Network Associates Laboratories. W ramach dostosowanej usługi PrimeSupport dostarczane są ogólne informacje o produktach i szybkie, niezawodne rozwiązania techniczne zapewniające niezawodne i nieprzerwane działanie. Stały rozwój i doskonalenie naszych technologii gwarantuje Network Associates Laboratories — światowy lider bezpieczeństwa i systemów informacyjnych.

networkassociates.com



YOUR NETWORK. OUR BUSINESS.™