



Ochrona prewencyjna – zmieniamy reguły

*Z bezpieczeństwem jest tak:
Jeśli nie działasz przed wystąpieniem
zagrożeń, możesz tylko reagować na skutki*





Wprowadzenie: Nowe reguły

13 sierpnia 2005 r. w Internecie pojawił się złośliwy robak o nazwie Zotob Bot. W ciągu kilku dni dołączyło do niego co najmniej kilkanaście innych robaków wykorzystujących lukę w funkcji Plug and Play w oprogramowaniu firmy Microsoft. Niektóre z nich były odmianami robaka Zotob, inne całkowicie się różniły. Atak dotknął m.in. największe koncerny medialne — CNN, ABC, NBC, Associated Press czy The New York Times.

Tylko jedna firma oferująca systemy zabezpieczeń była gotowa — przed wystąpieniem zagrożenia.

Opisane zdarzenie nieco drastycznie ilustruje problemy, przed jakimi stoją firmy intensywnie korzystające z Internetu, ale również sugeruje rozwiązanie. W przypadku robaka Zotob, podobnie jak we wcześniejszych dramatycznych atakach wirusów takich jak Sasser, Blaster czy Slammer, IBM Internet Security Systems miał już przygotowane skuteczne rozwiązania obronne. W ten sposób klienci firmy uniknęli jakichkolwiek szkód w sieci oraz zakłóceń w bieżącym funkcjonowaniu firmy — nie tylko przy pierwotnym ataku, ale również ze strony późniejszych odmian robaka.

To właśnie dzięki owej zdolności opracowywania „prewencyjnych” rozwiązań ochronnych IBM Internet Security Systems jest najbardziej zaufanym dostawcą systemów zabezpieczeń dla rządu USA i podległych mu agend oraz firm z listy Fortune 500. W odróżnieniu od konwencjonalnych metod ochrony, gdzie analiza i reakcja odbywa się dopiero po zaistnieniu ataku, ochrona prewencyjna zapobiega wystąpieniu zagrożeń, zanim w jakikolwiek sposób zaczną oddziaływać na sieć. Do niedawna IBM Internet Security Systems dostarczał swój system metodami ręcznymi, tzn. w sposób dość skomplikowany. Procedura udostępniania została jednak znacznie dopracowana i zautomatyzowana, a także umieszczona na prostej internetowej platformie, dzięki czemu ten naprawdę elitarny system zabezpieczeń jest teraz dostępny dla podmiotów różnej wielkości.

To kompleksowe rozwiązanie jest określane mianem platformy ochronnej IBM Internet Security Systems. Za jej pomocą IBM Internet Security Systems całkowicie zmienia zasady zapewnienia ciągłości działania firmy oraz zgodności z wymogami prawnymi/regulacyjnymi. Te nowe reguły podnoszą poprzeczkę w dziedzinie bezpieczeństwa, stając się praktycznie standardem odniesienia dla innych systemów zabezpieczeń:

- **„Prewencja” jest lepsza od „reakcji”.** Przy wyrafinowanych nowych formach ataków internetowych firma może ponieść znaczne straty już w kilka sekund. W takich warunkach prewencja ma absolutnie kluczowe znaczenie, ponieważ „reakcja” z definicji nie będzie wystarczająco szybka.
- **Problem z zapewnieniem bezpiecznego korzystania z Internetu nie leży w sieciach ani sprzęcie, ale w oprogramowaniu zainstalowanym w systemach ... a dokładniej mówiąc, w lukach w zabezpieczeniach tego oprogramowania.** Jeśli kluczem do skutecznej ochrony jest prewencja, to kluczem do prewencji jest umiejętność odnalezienia i zabezpieczenia luk, zanim zostaną one wykorzystane. Metody ochrony bazujące na reagowaniu na ataki (tradycyjny model ochrony antywirusowej polegający na analizie i opracowywaniu rozwiązań naprawczych już po zaistnieniu ataków) wciąż odgrywają pewną rolę, ale to właśnie metody bazujące na wcześniejszym wykrywaniu luk wyznaczają standardy efektywności systemów zabezpieczeń.
- **Prawdziwe bezpieczeństwo ma charakter dynamiczny — to nie jest przedmiot ani jedna z „funkcjonalności” infrastruktury.** Wraz z rosnącym stopniem komplikacji oprogramowania rośnie liczba i różnorodność zagrożeń. Od 1990 r. liczba aplikacji pracujących na serwerach i urządzeniach sieciowych rośnie w tempie wykładniczym, co oznacza równie szybkie pojawianie się nowych, zróżnicowanych zagrożeń. Aby system zabezpieczeń można było uznać za skuteczny, musi być on z góry na nie przygotowany. Ochrona prewencyjna oznacza podejmowanie działań przed wystąpieniem zagrożenia przez zastosowanie stale ewoluujących mechanizmów analitycznych oraz technik opracowanych w oparciu o bardzo nowatorskie i aktywne metody badawcze.
- **Ochrona prewencyjna – działanie przed wystąpieniem zagrożeń.** Ochrona prewencyjna została zaprojektowana tak, aby chronić firmę przed wystąpieniem potencjalnych zagrożeń
- **Prewencja redukuje koszty ochrony dzięki uproszczeniu obsługi systemu zabezpieczeń.** Firmy kupują rozwiązania technologiczne, aby ułatwić sobie życie, ale tradycyjne systemy zabezpieczeń (instalowanie poprawek, systemy wykrywania włamań, zapory sieciowe itd.) przysparzają pracy. Owa praca stanowi ponad połowę stale rosnących kosztów ochrony infrastruktury. Ograniczenie kosztów jest możliwe tylko dzięki udoskonaleniu systemów zabezpieczeń. Ochrona prewencyjna doskonale realizuje ten postulat.
- **Lepsze rozwiązanie.** Ochrona prewencyjna dostępna na zintegrowanej platformie pozwala wprowadzić kompleksowy system zabezpieczeń, który jest nie tylko bardziej skuteczny, ale również można go rozbudowywać oraz centralnie nim administrować.



Biznesowa potrzeba strategicznego podejścia do kwestii bezpieczeństwa Internetu

Obecnie Internet to podstawowe narzędzie wykorzystywane przez większość firm, co oznacza, że bezpieczeństwo korzystania z tego środka może decydować o ich sukcesach lub porażkach. Bezpieczeństwo Internetu ma ogromny wpływ na skuteczność zarządzania wewnętrznymi sieciami, wprowadzania nowych rozwiązań technicznych i aplikacji oraz przestrzegania nowych wymogów prawnych i branżowych standardów — i to wszystko w warunkach stale rosnącej różnorodności i wyrafinowania zagrożeń. Biorąc pod uwagę skalę problemu, zwykłe rozszerzenie zasięgu niedoskonałego systemu taktycznych i „reaktywnych” punktowych rozwiązań ochronnych nie jest żadnym wyjściem. Bezpieczeństwo użytkownika Internetu należy postrzegać jako absolutny wymóg w działalności firmy. Cel: Wprowadzenie skutecznych „prewencyjnych” rozwiązań ochronnych na zintegrowanej platformie, która obejmuje całą infrastrukturę organizacji (serwery, sieci i stacje robocze), daje się łatwo rozbudowywać, dostarcza informacji analitycznych umożliwiających podejmowanie odpowiednich działań oraz oferuje proste mechanizmy centralnego administrowania.

Wykraczanie poza tradycyjne przekonania i nieprzyjemne doświadczenia

Mimo całej uwagi i środków finansowych poświęconych na sprawy bezpieczeństwa obecne konwencjonalne rozwiązania wypaczają całą ideę ochrony. Często drogie i skomplikowane systemy zabezpieczeń przegrywają w starciu z jednym, nieprzewidzianym rodzajem ataku. W efekcie firmy są wciąż zmuszane do postawy reaktywnej — walki o naprawienie szkód i przywrócenie sprawności infrastruktury po zaistnieniu ataku. Bezpieczeństwo korzystania z Internetu wpływa praktycznie na wszystkie aspekty zarządzania, migracji do nowych rozwiązań technologicznych i rozwoju firmy, dlatego członkowie najwyższego kierownictwa muszą stale podnosić wymagania stawiane systemom ochrony przed zagrożeniami płynącymi z Internetu. Powinni oni żądać zabezpieczeń, które są skuteczne i łatwe w administrowaniu, a także postrzegać ich rolę w szerszym, bardziej strategicznym kontekście.

Poprawa ochrony sieci w celu zapewnienia wzrostu wydajności pracy

Od pewnego czasu obserwujemy intensywne poszerzanie zasięgu sieci firmowych — i to nie przez obejmowanie kolejnych oddziałów i pracowników zdalnych, ale również dostawców, klientów, podwykonawców, innych zewnętrznych instytucji oraz osób indywidualnych. Ponadto stale rozwijają się i upowszechniają nowe technologie takie jak łączność bezprzewodowa, inteligentne telefony czy wirtualne sieci prywatne. Postępująca integracja przynosi szereg wymiernych korzyści, m.in. skrócenie łańcuchów dostaw, szybsze reagowanie na oczekiwania klientów, zmniejszenie usterkowości i ogólne redukcję kosztów w różnych aspektach działalności. Niestety, konwencjonalne metody zabezpieczeń mogą sobie nie radzić z galopującym wzrostem liczby użytkowników sieciowych, powodując udostępnianie kluczowych systemów i danych „użytkownikom domyślnym”. Efektywny system ochrony internetowej powinien gwarantować zabezpieczenie infrastruktury ogólnofirmowej oraz umożliwiać rozszerzanie funkcjonalności sieci o rozwiązania wspomagające wzrost wydajności pracy, ograniczanie kosztów i skuteczną rywalizację na dynamicznym globalnym rynku.

Ochrona czegoś więcej niż tylko ciągłości działania sieci — ochrona optymalizacji wykorzystania jej przepustowości

Przestój w krytycznym momencie jest jak atak serca, co wyjaśnia, dlaczego osoby odpowiedzialne za działanie sieci tak bardzo starają się ich uniknąć. Z drugiej strony spadek przepustowości, który można przyrównać do chronicznej, ale mniej poważnej dolegliwości, jest regularnie tolerowany mimo osłabiającego wpływu na działanie przedsiębiorstwa. Ruch inicjowany przez nieuprawnione osoby i programy zajmuje pasmo potrzebne do obsługi aplikacji o podstawowym znaczeniu dla firmy.

Pogarsza efektywność działania sieci, zwiększa koszty obsługi infrastruktury i stwarza szereg dodatkowych zagrożeń dla bezpieczeństwa. Strategiczny system zabezpieczeń Internetu zawierający m.in. mechanizmy wykrywania anomalii i zapobiegania włamaniom, funkcjonujący na zintegrowanej platformie chroniący całą sieć począwszy od jej samego jądra, może zapobiec zarówno przestojom, jak i spadkowi przepustowości.

Bezpieczeństwo użytkownika Internetu należy postrzegać jako absolutny wymóg w działalności firmy.

Stosowanie nowych aplikacji bez wprowadzania nowych rodzajów ryzyka

Firmy regularnie stają w obliczu problemów z bezpieczeństwem wynikających z samej konstrukcji popularnych rozwiązań. Problemy te ulegają dodatkowemu wzmocnieniu na skutek szybkiego upowszechniania się coraz nowszych typów aplikacji, np. do komunikacji głosowej z wykorzystaniem protokołu IP (VoIP), zarządzania relacjami z klientami (CRM) itd. Wiele tych nowych technologii przyczynia się do powstania nowych luk w infrastrukturze informatycznej, stwarzając nowe punkty wejściowe czy bezpośrednio komunikując się z podstawowymi aplikacjami obsługi zaplecza. Podobnie jak w przypadku każdej kolejnej generacji rozwiązań technicznych, konwencjonalne systemy ochronne mają ograniczoną przydatność. Zadaniem systemów tradycyjnych jest zwalczanie znanych zagrożeń, podczas gdy zagrożenia tkwiące w najnowszych rozwiązaniach są przeważnie nieznanne. Właśnie dlatego strategiczny system ochrony internetowej musi opierać się na identyfikowaniu zagrożeń, a nie reagowaniu na już zaistniałe ataki. Nie ma możliwości przewidzenia wszystkich rodzajów ataków, jakie mogą być kierowane przeciw nowo powstającym aplikacjom. Doświadczenia pokazują jednak, że dzięki metodom aktywnej analizy i rozwojowi nowych technologii istnieje możliwość wykrywania i zabezpieczania luk (słabych punktów), do których prawdopodobnie będą kierowane ataki, oraz identyfikowania wzorców zachowań wskazujących na nowe, nieskatalogowane wcześniej ataki.



Kontrolowany rozrost sieci połączony z optymalizacją zarządzania zabezpieczeniami

Wraz z powiększaniem sieci zaczynają się w nich pojawiać setki, a nawet tysiące aplikacji i urządzeń mających chronić przed coraz bardziej różnorodnymi atakami — gdzie przeważnie owe aplikacje/urządzenia w ogóle się z sobą nie kontaktują ani nie koordynują swoich działań. Takie warstwy rozproszonych systemów istotnie zwiększają stopień komplikacji sieci oraz podnoszą koszty zarządzania nimi i ich obsługi.

Ponadto taki konglomerat taktycznych uzupełnień nie jest w stanie zapewnić odpowiedniej ochrony całości infrastruktury, ponieważ nie rozwiązują one fundamentalnych słabości na poziomie ogólnofirmowym. Wręcz przeciwnie — stanowią nieomal zaproszenie dla potencjalnych napastników:

- *Funkcjonalne „białe plamy” między autonomicznymi produktami tworzą idealne punkty wejściowe dla wirusów i podobnych obiektów.*
- *Brak spajającej bazy architektonicznej lub technologicznej, która ułatwiałaby wdrażanie aplikacji.*
- *Brak centralnego obrazu i możliwości zarządzania różnymi produktami umożliwiającymi efektywne sterowanie funkcjami i prowadzenie dla nich rejestrów zdarzeń oraz niezdolność podawania dokładnych informacji sprawozdawczych wymaganych przez przepisy prawa.*

Tu również odpowiedzią jest strategiczne, „platformowe” podejście do kwestii zabezpieczenia przed zagrożeniami internetowymi. Z samej definicji platforma umożliwia przyszłe rozszerzenie — o nowych użytkowników i fizyczne lokalizacje — bez spadku wydajności działania ani istotnego wzrostu stopnia komplikacji zarządzania.

Skuteczny system ochrony ułatwia spełnienie wymogów regulacyjnych

Konieczność spełnienia wymogów regulacyjnych znacznie podnosi oczekiwania wobec nowoczesnego systemu ochrony internetowej. HIPAA, ustawa Sarbanes’a-Oxley’a, Nowa Umowa Bazylejska czy ustawa Gramm-Leach-Bliley mogą skutkować różnymi zobowiązaniami prawnymi i finansowymi. Ponadto ujawnienie przypadków nieprzestrzegania któregokolwiek z wymaganych przepisów lub ukrywania naruszenia zabezpieczeń systemów firmy może spowodować negatywny odbiór społeczny i utratę przychodów lub pogorszenie wizerunku.

Pod względem strategicznym system ochrony internetowej powinien sprawić, że przestrzeganie wymogów regulacyjnych będzie niejako oczywiste z dwóch względów:

- *Przy sprawnym systemie ochrony nie powinny występować żadne naruszenia zabezpieczeń.*
- *Platformowa konstrukcja systemu ochrony internetowej powinna automatycznie oferować funkcje wglądu w dane i sprawozdawczości umożliwiające dokumentowanie zdarzeń na potrzeby kontroli.*

Ulotny święty grał bezpieczeństwa

Część firm na całym świecie będzie zapewne dalej funkcjonować w fałszywym przekonaniu, że ich konwencjonalne systemy zapewniają wystarczającą ochronę. Inne mogą przestać na popularnym przekonaniu, że pewnego ryzyka nie da się po prostu uniknąć, tzn. że możliwa jest tylko reaktywna ochrona.

Idealistyczna wizja bezpieczeństwa mówi o rozwiązaniu, które będzie w stanie powstrzymać zagrożenia przed ich dotarciem do systemów firmy — prewencyjne zapobieganie tak znanym, jak i nieznanym atakom w sposób niedrogi i całkowicie automatyczny.

W rzeczywistości owa wizja jest całkowicie realna. Wymaga po prostu stworzenia zintegrowanej platformy z funkcjami działań prewencyjnych i zaawansowanymi mechanizmami wyszukiwania luk. To jedyna realistyczna strategia, ponieważ zapewnia realizację trzech podstawowych wymogów:

- *Skutecznie chroni przed szkodami spowodowanymi naruszeniem zabezpieczeń.*
- *Umożliwia planowanie systemów zabezpieczeń i zarządzanie nimi w sposób długofalowy przez stworzenie platformy wspierającej stale ewoluujące rozwiązania techniczne.*
- *Zawiera narzędzia pozwalające oferować gwarantowaną ochronę dzięki usługom zabezpieczeń udostępnianym „na żądanie”.*

Weryfikacja poglądów na temat zadań systemów zabezpieczeń

Na poziomie funkcjonalnym problemy z zapewnieniem bezpieczeństwa przypominają cieknący dach przy coraz silniejszym deszczu. Pytanie brzmi: Czy w celu powstrzymania przecieku i usunięcia szkód wybierzesz rozwiązanie, które próbuje analizować poszczególne spadające krople, czy też takie, które odszuka i naprawi dziurę w dachu?

Na poziomie strategicznym problem polega na stworzeniu takiego systemu ochrony, który będzie wykraczał poza łatanie dziur w dachu. Pytanie brzmi: Jak informacje zebrane przez system ochrony wykorzystać z pożytkiem dla firmy?

Aby naprawdę zrozumieć charakter zagrożeń dla bezpieczeństwa, wystarczy przyjrzeć się używanemu oprogramowaniu przypominającemu... szwajcarski ser

Firmy używają najróżniejszych aplikacji: biurowych, do obsługi funkcji zaplecza, sieciowych systemów operacyjnych itd. Praktycznie wszystkie programy mają luki, tzn. błędy w kodzie źródłowym. Wraz ze wzrostem stopnia komplikacji programów i pojawiania się coraz to nowych wersji oraz wydań dramatycznie rośnie ilość kodu, a co za tym idzie — błędów. Stosując analogię do przykładu z deszczem, owe luki to „dziury w dachu”. Rosnąca liczba luk w oprogramowaniu prowadzi do jeszcze szybszego wzrostu liczby zagrożeń, ponieważ teoretycznie każda luka może być celem różnych form ataków. Wiele z tych metod cechuje się bardzo dużym stopniem wyrafinowania i szkodliwości.



Wyszukiwanie luk to jeden z kluczowych mechanizmów zawartych w nowatorskiej platformie ochrony prewencyjnej opracowanej przez IBM Internet Security Systems. Dzięki identyfikowaniu luk przed wystąpieniem ataków system IBM Internet Security Systems oferuje nieosiągalny dla innych systemów poziom ochrony przed najważniejszymi zagrożeniami internetowymi. Technologia IBM Internet Security Systems Virtual Patch™ eliminuje konieczność tak częstego awaryjnego instalowania aktualizacji, chroniąc „dziurawe” oprogramowanie do czasu, aż trwałe (docelowe) aktualizacje zostaną sprawdzone i zainstalowane w ramach zwykłej, planowanej obsługi serwisowej. W przykładzie z deszczem technologia Virtual Patch przypomina ochronną plandekę zabezpieczającą cieknący dach do czasu, aż użytkownik dokona niezbędnych napraw w dogodnym dla siebie terminie.

Przy prewencji jako fundamencie platforma ochronna generuje dane analityczne przydatne w różnych aspektach działania firmy

Konstrukcja platformy ochronnej IBM Internet Security Systems umożliwia centralny wgląd i administrowanie całą infrastrukturą zabezpieczeń istniejącą w przedsiębiorstwie. Dzięki temu bezpieczeństwo może stanowić jeden z kluczowych zasobów firmy.

System ten ma na celu:

- *Wykrywanie i oznaczanie luk oraz podejmowanie wobec nich odpowiednich działań zabezpieczających.*
- *Oznaczanie elementów systemu zabezpieczeń i centralne zarządzanie tymi składnikami.*
- *Wykrywanie i dokumentowanie nowych użytkowników.*
- *Optymalizacja wykorzystania przepustowości sieci.*
- *Dokumentowanie i zgłaszanie warunków i zdarzeń dotyczących bezpieczeństwa.*
- *Zarządzanie poprawkami w ramach rutynowej obsługi serwisowej.*
- *Sprawne udostępnianie informacji dotyczących bezpieczeństwa między działami i obszarami funkcjonalnymi.*
- *Zmniejszenie liczby zgłoszeń do działu pomocy technicznej.*
- *Sprawniejsze testowanie i weryfikowanie nowych aplikacji przed wdrożeniem w skali całego przedsiębiorstwa.*
- *Wdrażanie aplikacji ochronnych i zarządzanie nimi na jednej wspólnej platformie.*
- *Sprawniejsza realizacja procesów zarządzania ryzykiem.*

Platforma ochronna opracowana przez IBM Internet Security Systems

- **Poprawa dostępności i niezawodności sieci.**

IBM Internet Security Systems jest szczególnie dobrze przygotowany do budowy kompleksowych systemów ochronnych bazujących na mechanizmach prewencji, ponieważ dysponuje trzema podstawowymi elementami:

- 1) znakomity dział badawczo-rozwojowy,
- 2) globalny zasięg działalności,
- 3) zintegrowana platforma ochronna.

IBM Internet Security Systems obecnie jest jedną z czołowych firm zajmujących się badaniami nad systemami zabezpieczeń i wprowadzaniem innowacji w tym zakresie — to właśnie IBM Internet Security Systems opracował technologie identyfikowania luk w oprogramowaniu, wykrywania włamań i zapobiegania atakom. Dlatego na tle innych dostawców systemów zabezpieczeń IBM Internet Security Systems jest szczególnie dobrze przygotowany do budowy systemów prewencyjnych

tak potrzebnych dzisiejszym firmom intensywnie korzystającym z Internetu. Połączenie jednostki badawczo-rozwojowej IBM Internet Security Systems X-Force®, globalny zasięg centrów operacyjnych i usług outsourcingowych oraz znakomita platforma ochronna IBM Internet Security Systems tworzą najbardziej zaawansowane i kompletne warunki do budowy systemów zabezpieczeń, wprowadzając funkcje ochrony prewencyjnej tak dotąd zaniedbywane przez rynek.

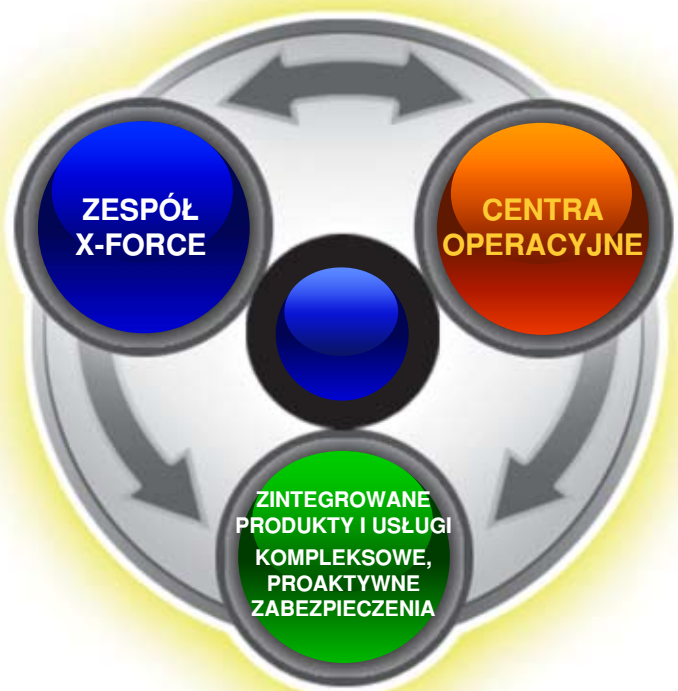
IBM Internet Security Systems X-Force — forpocztą badawczo-rozwojowa

Aktywne, dogłębne badania nad zabezpieczeniami są — i zawsze były — podstawą działania IBM Internet Security Systems oraz produktów i usług oferowanych przez firmę. Zespół badawczo-rozwojowy X-Force® (X-Force) stosuje nowatorskie metody badawcze ukierunkowane na aplikacje biznesowe, aplikacje zaplecza i sieciowe systemy operacyjne tworzące stale ewoluującą infrastrukturę wspomagania sprzedaży. Ten niezrównany zasób informacji o brakach w zabezpieczeniach różnych programów stanowi fundament systemów ochrony prewencyjnej tworzonych przez firmę.

Centra operacyjne IBM Internet Security Systems — nasze „ucho przy ziemi”

Dwadzieścia cztery godziny na dobę, każdego dnia IBM Internet Security Systems zarządza infrastrukturą zabezpieczeń wielu najbardziej wyczulonych na tym punkcie firm i agend rządowych na całym świecie. Nadzorowanie setek sieci rozproszonych po całym świecie daje nam dokładne informacje o zjawiskach i zdarzeniach zachodzących w Internecie, ułatwiając identyfikowanie nowych możliwości ataków. Specjaliści zatrudnieni w centrach operacyjnych na całym świecie analizują wymianę komunikatów i podejrzany ruch w sieci. Obserwują i analizują techniki ataków, ucząc się jednocześnie ich odtwarzania, przewidywania i zatrzymywania.

IBM INTERNET SECURITY SYSTEMS





Platforma ochronna IBM Internet Security Systems — nowy standard

W postaci platformy ochronnej IBM Internet Security Systems stworzył proste, całkowicie zintegrowane rozwiązanie, które stawia mechanizmy prewencyjnego zabezpieczania w zasięgu wszystkich instytucji dbających o bezpieczeństwo.

IBM Internet Security Systems oferuje całą rodzinę zaawansowanych aplikacji i usług, mogących pracować autonomicznie lub razem w postaci modułowego, zintegrowanego systemu. Platforma ochronna IBM Internet Security Systems to kompletny i niezwykle zaawansowany pakiet narzędzi tworzący w pełni kompleksowe rozwiązanie. Oprócz zaawansowanych funkcji zapobiegania włamaniom, wykrywania anomalii, zapory sieciowej, obsługi wirtualnych sieci prywatnych, skanowania w poszukiwaniu luk oraz ochrony antywirusowej zawiera także znacznie usprawnione mechanizmy ochrony poczty elektronicznej i filtrowania zawartości stron internetowych. Ponadto jest w stanie objąć całą infrastrukturę w firmie, oferując rozwiązania przeznaczone dla stacji roboczych, serwerów, sieci i bram. Wszystkimi aplikacjami zabezpieczeń dostępnymi na platformie można bez problemu zarządzać z dowolnego miejsca.

Platforma ochronna IBM Internet Security Systems jest dostarczana klientom na dwa sposoby. Mogą oni wybrać między samodzielną instalacją i konfiguracją, a bezpośrednim monitorowaniem i zarządzaniem całą infrastrukturą sieciową w firmie przez IBM Internet Security Systems.

Rewolucyjna architektura oferująca kompleksowe zabezpieczenie:

- ***Jeden zbiorczy wgląd w całą sieć (ułatwiający przestrzeganie wymogów regulacyjnych i sprawozdawczość)***
- ***Skalowalna platforma i usługi***
- ***Korelacja i integracja wielu źródeł danych***
- ***Elementy infrastruktury najlepsze w swojej klasie***
- ***Możliwość współdziałania z najnowocześniejszymi rozwiązaniami technicznymi (np. Anomaly Detection Service)***
- ***Zarządzanie zabezpieczeniami na zasadach outsourcingu w trybie 24/7***
- ***Ograniczenie przestoju i optymalizacja działania systemów bez istotnych inwestycji w technologie ani personel***
- ***Usługi gwarantowanej zdalnej ochrony***

Podsumowanie

Przedsiębiorstwa, w których działalności Internet odgrywa kluczową rolę, nie mogą sobie już pozwolić na poleganie na metodach ochrony reaktywnej. Ryzyko ogromnych strat spowodowanych przez wyrafinowane ataki, nowe wymagania regulacyjne oraz gwałtownie rosnące koszty zarządzania przestarzałymi systemami zabezpieczeń są poważnym ostrzeżeniem dla kierownictwa. Jedyną strategią, która skutecznie rozwiązuje te problemy, jest ochrona prewencyjna. Ochrona taka wymaga niezwykle zaawansowanych metod badawczych, uważnego wychwytywania tendencji i metod ataków oraz jednolitej i rozsądnej cenowo platformy, na której będą działały specjalistyczne aplikacje bazujące na zgromadzonej wiedzy. Ochrona prewencyjna to jedyny model rozwiązań, w którym użytkownicy dbający o bezpieczeństwo mogą rzeczywiście interweniować przed wystąpieniem zagrożenia. Aktualnie IBM Internet Security Systems jako jedyny na świecie może dostarczać takie rozwiązania. Dysponuje rozległą wiedzą, nowatorskimi metodami badawczymi i rozwiązaniami technicznymi potrzebnymi zarówno do budowy systemów, jak i udostępniania ich w formie łatwych w obsłudze urządzeń i programów lub na zasadzie outsourcingu.

Informacje o IBM Internet Security Systems

IBM Internet Security Systems to zaufany doradca w dziedzinie zabezpieczeń dla tysięcy najważniejszych światowych firm i agend rządowych, oferujący systemy prewencyjnej ochrony sieci, serwerów i stacji roboczych. Uznany lider w swoim sektorze, oferuje zintegrowaną dedykowaną platformę chroniącą przed znanymi i nieznanymi zagrożeniami, zapewniającą niezakłócone działanie sieci oraz zabezpieczającą użytkowników przed atakami internetowymi zanim jeszcze uderzą one w infrastrukturę. Produkty i usługi oferowane przez IBM Internet Security Systems bazują na informacjach analitycznych gromadzonych przez zespół badawczo-rozwojowy X-Force — niekwestionowany światowy autorytet w dziedzinie badań nad brakami w zabezpieczeniach programów i zagrożeniami. Linie produktów ochrony prewencyjnej uzupełniają kompleksowe usługi IBM Managed Security Services.

Aby uzyskać więcej informacji o rozwiązaniach IBM Internet Security Systems i systemach ochrony prewencyjnej, odwiedź stronę:

ibm.com/pl/services



IBM Polska Sp. z o.o.

Wiśniowy Business Park
Ul. 1 Sierpnia 8
02-134 Warszawa
tel. +48 22 878 6777
fax: +48 22 878 6888

Wyprodukowano w Polsce
Wszystkie prawa zastrzeżone

IBM i logo IBM są zastrzeżonymi znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach.

Ahead of threat, Virtual Patch oraz X-Force są zastrzeżonymi znakami towarowymi Internet Security Systems, Inc. w Stanach Zjednoczonych i/lub innych krajach. Internet Security Systems, Inc. jest spółką całkowicie zależną od firmy International Business Machines Corporation.

Nazwy innych firm, produktów i usług mogą być znakami towarowymi lub znakami usług należącymi do innych podmiotów.

Referencje dotyczące produktów i usług IBM zawarte w niniejszej publikacji nie oznaczają, że IBM zamierza udostępnić je we wszystkich krajach, w których działa IBM.

* Gwarancja zwrotu pieniędzy (dla usług zdalnej ochrony — wyłącznie poziom Premium):
Jeśli firma IBM Internet Security Systems nie wypełni swoich zobowiązań z tytułu gwarancji zapobiegania naruszeniom zabezpieczeń w którymkolwiek miesiącu kalendarzowym, konto Klienta zostanie uznane pełną miesięczną kwotą właściwej miesięcznej opłaty monitoringowej za każde zdarzenie niewypełnienia tych zobowiązań. Szczegółowe informacje znajdują się w umowie świadczenia usług przez IBM Internet Security Systems.