

## IBM oferuje ochronę przed wyrafinowanymi i złożonymi zagrożeniami bezpieczeństwa dla środowiska informatycznego

*Pakiet usług IBM służących minimalizacji zagrożeń*



# CORAZ POWAŻNIEJSZE ZAGROŻENIA. CORAZ LEPSZE ODPOWIEDZI.

## Nie tak dawno temu typowa sieć informatyczna miała zaledwie parę luk i groziło jej tylko kilka form ataku.

Ruch mierzono w megabitach. Aplikacje służyły do obsługi poczty elektronicznej i przeglądania zasobów Internetu, a domyślną akcją dla polityki bezpieczeństwa było „blokuj”.

Po czym stopień złożoności działań firm i infrastruktury informatycznej zaczął rosnąć — w tempie wykładniczym. Równolegle, równie szybko zaczęły się pojawiać nowe luki i zagrożenia.

Obecnie w sieciach są przesyłane gigabajty danych. Aplikacje sieciowe często stanowią jądro funkcjonowania przedsiębiorstwa, a zasady polityki bezpieczeństwa przewidują domyślne zezwolenie na dostęp. Efekt? Ogromna podatność na ataki. Tysiące potencjalnych celów i komercjalizacja zagrożeń bezpieczeństwa. Rośnie częstotliwość ataków wykorzystujących luki w zabezpieczeniach, a ich forma przybiera nieznaną dotąd poziom szkodliwości. Ataki mogą być bardzo dyskretne, a jednocześnie bardzo dotkliwe.

## Atak przebiega bardzo szybko. Zabezpieczenia muszą dotrzymać mu kroku.

Jak firma może się bronić? Reakcja po ataku nie wystarczy. Po wykryciu luki możliwe jest jej wielokrotne wykorzystanie. Nowoczesne ataki przebiegają bardzo szybko, dlatego trzeba być na nie przygotowanym już wcześniej.

Jest jednak mało prawdopodobne, aby większość firm poradziła sobie z tym wyzwaniem samodzielnie. Zapewnienie bezpieczeństwa przez 24 godziny na dobę 7 dni w tygodniu może wymagać zaangażowania od 6 do 9 osób — tylko dla jednego stanowiska. Nawet jednak gdy personel jest dostępny, zapewnienie

odpowiedniego poziomu ochrony wymaga dysponowania wyrafinowanymi narzędziami i umiejętnościami, możliwości reagowania na incydenty oraz dogłębnej znajomości najnowszych form ataków, trendów i technologii.

Ponadto rozwiązania o wąskiej specjalizacji nie są w stanie chronić przed nowymi złożonymi typami zagrożeń. Obecne zintegrowane środowiska wymagają kompleksowych i zaawansowanych metod zabezpieczeń, a także aktywnych metod prewencyjnej minimalizacji zagrożeń.

## Kompleksowy pakiet rozwiązań ochronnych IBM.

IBM Internet Security Systems™ (ISS) oferuje zintegrowany pakiet rozwiązań mających na celu ochronę infrastruktury wspierającej działalność operacyjną przedsiębiorstw. Pakiet zawiera także rozbudowane funkcje administracyjne umożliwiające skuteczne zarządzanie zabezpieczeniami.

IBM oferuje całościowe rozwiązanie oparte na najwyższej klasy usługach konsultingowych i outsourcingowych. Wyjątkowa wartość tych usług jest rezultatem wsparcia ze strony najlepszego w branży zespołu badawczo-rozwojowego oraz umiejętności IBM w dziedzinie precyzyjnego ustalania potrzeb i tworzenia zintegrowanych produktów/usług. Rozwiązania dostarczane przez IBM koncentrują się na pięciu podstawowych obszarach:

- **Usługi zabezpieczania danych:** pomagają chronić dane przed zagrożeniami w trakcie przesyłania oraz składowania
- **Usługi służące minimalizacji zagrożeń:** pomagają firmom zapobiegać zagrożeniom dzięki ochronie sieci i punktów końcowych, zabezpieczeniom pozwalającym zachować integralność aplikacji oraz usługom zarządzania lukami w oprogramowaniu
- **Usługi ochrony fizycznej:** umożliwiają integrację systemu cyfrowego





>>>ORGANIZED CRIME

nadzoru wizyjnego z siecią i systemami informatycznymi

- **Usługi zarządzania tożsamością i dostępem:** projektowanie, instalacja, wdrażanie i serwisowanie zintegrowanego systemu zarządzania tożsamością
- **Usługi weryfikacji polityki zabezpieczeń:** ocena istniejących procedur dotyczących bezpieczeństwa w kontekście potrzeb biznesowych

### Aktywna prewencyjna ochrona

Przy stratach finansowych, jakie wielu firmom wciąż wyrządza różne szkodliwe oprogramowanie, usługi IBM służące minimalizacji zagrożeń mogą pomóc dopasować infrastrukturę zabezpieczeń do unikatowych potrzeb przedsiębiorstwa. IBM koncentruje się na 4 obszarach mających zagwarantować bezpieczny dostęp i ochronę:

- **Ochrona sieci:** umożliwia całościowe zapobieganie zagrożeniom oraz ich wykrywanie
- **Ochrona punktów końcowych:** opieka nad punktami końcowymi sieci oraz systemy zdalnego dostępu wyposażone w zaawansowane funkcje bezpieczeństwa
- **Bezpieczeństwo aplikacji:** pomoc w zabezpieczeniu aplikacji i danych w celu poprawy ogólnego stanu bezpieczeństwa
- **Zarządzanie bezpieczeństwem i lukami w oprogramowaniu:** aktywne identyfikowanie informacji o stanie bezpieczeństwa systemów firmy i przestrzeganiu wymogów regulacyjnych oraz odpowiednie zarządzanie zagadnieniami w tych obszarach

### Błyskawiczna ochrona — realizowana wirtualnie

Unikatowym składnikiem systemu oferowanego przez IBM jest funkcjonalność Virtual Patch®, która pozwala chronić

zasoby informatyczne jeszcze przed zainstalowaniem poprawek. Jeśli skanowanie sieci ujawni istnienie luk, analityk z IBM ISS może zapewnić ochronę całej sieci lub wybranych serwerów przez zablokowanie możliwości wykorzystania luki do momentu zainstalowania poprawki. Takie rozwiązanie znacznie poprawia ogólną sprawność działania firmy i obniża koszty.

Łącznie usługi zawarte w pakiecie stanowią zintegrowany system zabezpieczeń wspomagany przez rozległe działania badawczo-rozwojowe. Ponadto są dostarczane w sposób zapewniający przedsiębiorstwom możliwość wyboru i elastyczność w pozyskiwaniu składników systemu ochrony.

### Zespół badawczo-rozwojowy X-Force

Motorem napędowym usług IBM z zakresu bezpieczeństwa jest zespół badawczo-rozwojowy X-Force® działający w ramach IBM Internet Security Systems. To jedna z najlepszych jednostek tego typu na świecie. Prace zespołu koncentrują się na analizowaniu i badaniu luk oprogramowania w celu opracowania prewencyjnych rozwiązań ochronnych.

Dzięki dokładnemu rozpoznaniu narzędzi i metod konstruowania ataków zespół jest w stanie przygotować produkty chroniące przed całymi kategoriami zagrożeń, a nie tylko indywidualnymi atakami. Proces badawczo-rozwojowy obejmuje identyfikację i analizę luk, zebranie informacji z różnych innych źródeł badawczych, ciągłe monitorowanie i analizowanie zagrożeń internetowych na całym świecie oraz błyskawiczne powiadamianie o pojawiających się aktualnie zagrożeniach.

### Usługi konsultingowe dla systemów zabezpieczeń

Pakiet usług konsultingowych dla systemów zabezpieczeń obejmuje wszystkie

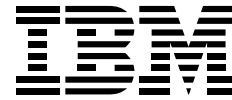
aspekty działań związanych z minimalizacją zagrożeń – od projektowania architektury i infrastruktury, przez opracowywanie polityki bezpieczeństwa, audyt, wspomaganie wewnętrznego personelu klienta, aż do pomocy w przestrzeganiu wymogów regulacyjnych.

Konkretne usługi mogą dotyczyć np. oceny zgodności ze standardem PCI (Payment Card Industry), analizy braków w realizacji normy ISO (International Organization for Standardization) 17799 czy przestrzegania norm branżowych i ustawowych — np. usługi pomagające zapewnić przestrzeganie przepisów FFIEC (Federal Financial Institutions Examination Council), federalnej ustawy o zarządzaniu bezpieczeństwem informacji (Federal Information Security Management Act, FISMA), ustawy Gramma-Leacha-Blileya, ustawy o ciągłości i rozliczaniu ubezpieczenia zdrowotnego (Health Insurance Portability and Accountability Act, HIPAA), ustawy Sarbanesa-Oxleya itd.

### Usługi zarządzania bezpieczeństwem

IBM oferuje również kompleksowy pakiet usług zdalnego zarządzania bezpieczeństwem dla sieci, serwerów i stacji roboczych, ale także dla systemów wykrywania włamań i zapobiegania włamaniom, zapór ogniowych, wirtualnych sieci prywatnych, systemów poczty elektronicznej i usług internetowych.

Celem usług zarządzania bezpieczeństwem jest szybkie zapewnienie odpowiedniego poziomu bezpieczeństwa, który umożliwi firmom poprawę ciągłości funkcjonowania i wydajności pracy oraz utrzymanie/poprawę stopnia przestrzegania różnych ustawowych wymogów. Analizy IBM pokazały, iż usługi zarządzania bezpieczeństwem mogą przynieść redukcję kosztów rzędu nawet 55%.



## Dlaczego IBM?

Szeroki zestaw produktów i pakiet usług konsultingowych oraz outsourcingowych oferowanych przez IBM zapewnia skuteczną minimalizację zagrożeń w otoczeniu, gdzie ataki są coraz lepiej zorganizowane, wyrafinowane i złożone.

Produkty IBM współpracujące z systemami różnych producentów umożliwiają nieprzerwane korzystanie z całościowego systemu ochrony. Zespół X-Force — jednostka badawczo-rozwojowa, której dokonania leżą u podstaw wszystkich produktów i usług — to jedna z najbardziej szanowanych na świecie organizacji zajmujących się badaniem problematyki bezpieczeństwa. Ponadto IBM ISS oferuje umowy świadczenia usług (SLA) przewidujące proporcjonalne rekompensaty za nieskuteczność ochrony, tzn. zwraca w gotówce kwotę 50 tys. USD za każde

naruszenie zabezpieczeń spowodowane skutecznym atakiem wymienionym na liście rozpoznanych ataków prowadzonej przez zespół X-Force®. \*

## Więcej informacji

Aby dowiedzieć się więcej o usługach oferowanych przez IBM Internet Security Systems oraz usługach służących minimalizacji zagrożeń, skontaktuj się z przedstawicielem handlowym IBM lub odwiedź następującą witrynę:

[ibm.com/pl/services](http://ibm.com/pl/services)

## IBM Polska Sp. z o.o.

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

Wyprodukowano w Polsce  
Wszystkie prawa zastrzeżone

IBM, logo IBM, BladeCenter, Internet Security Systems, Proventia, Rational, SiteProtector, System p, System z, Tivoli, Virtual Patch i X-Force są znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach.

Nazwy innych firm, produktów lub usług mogą być ich znakami towarowymi lub znakami usługowymi.

Zawarte w tym dokumencie odniesienia do produktów lub usług IBM nie oznaczają, że są one dostępne we wszystkich krajach, w których działa IBM.

---

\* Zwrot pieniędzy (dla usług zdalnej ochrony oferowanych przez IBM — wyłącznie poziom Premium): Jeśli IBM Internet Security Systems nie wypełni swoich zobowiązań z tytułu gwarancji zapobiegania naruszeniom zabezpieczeń, klient otrzyma 50 tys. USD za każdy przypadek niewypełnienia tych zobowiązań. Szczegółowe informacje znajdują się w umowie świadczenia usług przez IBM Internet Security Systems.

**IBM oferuje kompletne systemy zabezpieczeń oczekiwane przez dzisiejsze przedsiębiorstwa, budując je na bazie różnorodnych usług, oprogramowania i sprzętu:**

### Usługi

- Audyt bezpieczeństwa
- Usługi zapobiegania zagrożeniom i ich minimalizacji — IBM ISS
- Usługi zarządzania bezpieczeństwem
- Nadzór z wykorzystaniem cyfrowego przekazu wideo
- Usługi zarządzania tożsamością i dostępem
- Usługi dotyczące przestrzegania wymogów regulacyjnych
- Usługi zabezpieczania danych

### Oprogramowanie

- IBM Rational® Method Composer
- Pakiet oprogramowania IBM Tivoli®
- Pakiet oprogramowania IBM Proventia®
- Pakiet oprogramowania Consul

### Sprzęt

- Serwery IBM System z™, IBM System p™ i IBM BladeCenter®
- Urządzenia sieciowe Proventia