

Usługi zdalnego zarządzania bezpieczeństwem infrastruktury IT – IBM Managed Security Services

Na czym polega skuteczna ochrona

Ochrona zasobów informacyjnych i systemów IT powinna pracować w trybie 24x7x365. Bardzo mało firm może pozwolić sobie na zatrudnienie odpowiedniej ilości profesjonalistów, aby można było w trybie ciągłym monitorować stan bezpieczeństwa sieci oraz we właściwym czasie skutecznie reagować na pojawiające się ataki. Hakerzy wykorzystują niedoskonałości oprogramowania, słabości protokołów komunikacyjnych, błędy konfiguracyjne itd. Zatem głównym celem ochrony powinno być przeciwdziałanie atakom bazującym na tych lukach.

Skuteczna ochrona wymaga dostępu do pełnej wiedzy o najnowszych technikach włamań. Bez tej wiedzy z perspektywy wewnętrznej sieci trudno oszacować ryzyka związane z konkretnym atakiem, a nawet odróżnić nietypowy ruch w sieci od działań hakerów. Częste pomyłki mogą prowadzić do blokowania właściwych pakietów, powodując opóźnienia, a nawet zatrzymanie procesów biznesowych i niezadowolenie klientów.

Należy też pamiętać o zagrożeniu natury psychologicznej. Zwykle przedsiębiorstwa łatwiej wydają pieniądze na zakup produktów związanych z bezpieczeństwem niż na proces zarządzania systemem bezpieczeństwa zbudowanego z tych produktów. Taka dysproporcja nie sprzyja ani skuteczności ochrony systemów IT ani optymalizacji kosztów.

Managed Security Services

Usługi Managed Security Services (MSS) polegają na powierzeniu profesjonalnej firmie całości lub części procesu zarządzania bezpieczeństwem infrastruktury teleinformatycznej.

Usługi MSS obejmują proces zarządzania, dostęp do zasobów wiedzy i konsultacje z najlepszymi ekspertami. Większość ofert usług MSS dostępnych na rynku obejmuje tylko monitorowanie bezpieczeństwa wybranych urządzeń sieciowych. Jednak praktycznie żadna oferta nie zapewnia w pełni kompleksowego systemu ochrony, którego skuteczność jest gwarantowana karami pieniężnymi. Poza zdalnym zarządzaniem podsystemami bezpieczeństwa IT usługi MSS obejmują także regularne sprawdzanie podatności sieci i serwerów na najnowsze metody ataków.

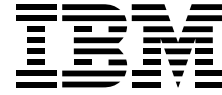
Usługi IBM Managed Security Services (MSS) bazują na wiedzy i doświadczeniu laboratorium badawczego X-Force, które jest czołową komercyjną organizacją zajmującą się zagrożeniami ze strony Internetu i lukami zabezpieczeń. X-Force monitoruje trendy w Internecie i gromadzi informacje o problemach bezpieczeństwa z ponad 5000 źródeł w tym ze środowisk hakerów. Prowadzona przez X-Force lista publicznie znanych ataków zawiera dane wszystkich najgroźniejszych ataków i jest regularnie aktualizowana.

Ocenia się, że od 1996 r. X-Force we współpracy z innymi laboratoriami badawczymi, wykrył więcej poważnych luk w oprogramowaniu niż wszystkie pozostałe podmioty komercyjne razem wzięte. Specjalistyczna wiedza X-Force jest bazą, na której zbudowano usługi MSS.

Powierzenie profesjonalistom procesu zarządzania bezpieczeństwem ma wiele zalet:

- *system bezpieczeństwa jest zarządzany non-stop w trybie 24x7x365*
- *zapewniony jest bardzo wysoki poziom skuteczności przeciwdziałania atakom*
- *jakość i skuteczność procesu zarządzania jest mierzona obiektywnymi wskaźnikami zdefiniowanymi w SLA*
- *bardzo mała liczba błędów w ocenie szkodliwości wykrytych incydentów*
- *koszty związane z zarządzaniem bezpieczeństwem IT są proporcjonalne do ilości zarządzanych elementów i zakresu funkcjonalności, a nie do ilości etatów*
- *skuteczność przeciwdziałania atakom jest gwarantowana karami pieniężnymi określonymi w umowie na świadczenie usługi*

IBM MSS to profesjonalna usługa z gwarantowaną skutecznością ochrony systemów przedsiębiorstwa przed zagrożeniami płynącymi z Internetu, której cena jest tylko ułamkiem kosztów zasobów koniecznych do samodzielnego zarządzania.



Zakres usługi precyzyjnie dopasowany do potrzeb klienta

Oferta IBM ISS umożliwia szeroki wybór opcji w zakresie ochrony, jej funkcjonalności i rodzaju wsparcia analitycznego. Poniżej są opisane najbardziej typowe opcje usług IBM MSS.

Usługa kompleksowej ochrony sieci — Całodobowa ochrona sieci w trybie 24x7x365 obejmuje zarządzanie firewallem, wykrywanie włamań na podstawie sond IDS, ochronę antywirusową na styku z Internetem, ochronę antyspamową, blokowanie stron WWW oraz bezpieczny zdalny dostęp poprzez VPN.

Usługa ochrony serwerów — Usługa jest realizowana w czasie rzeczywistym w trybie 24x7x365 i polega na wykrywaniu włamań i nieautoryzowanych działań w serwerach różnych platform. Do monitorowania zagrożeń używa się sond oprogramowania IDS RealSecure.

Usługa ochrony stacji roboczych — Usługa jest realizowana w czasie rzeczywistym w trybie 24x7x365 i polega na monitorowaniu zagrożeń stacji roboczych i reagowaniu na nie. Zakres usługi poza kompleksową ochroną stacji może także obejmować monitorowanie wypełniania różnorodnych wymogów regulacyjnych.

Usługa zarządzania firewallem i zdalnym dostępem — Całodobowa usługa polega na zdalnym zarządzaniu pracą firewalla oraz monitorowaniu bezpiecznego zdalnego dostępu przez VPN.

Usługa wykrywania luk zabezpieczeń — Usługa obejmuje regularne skanowanie serwerów i urządzeń sieciowych klienta dostępnych z Internetu. Poza skanowaniem usługa obejmuje analizę wykrytych luk, gotowe propozycje ich usunięcia oraz bezpośrednią pomoc ekspercką w ich usuwaniu.

Unikalność usługi IBM MSS

Gwarancja skuteczności — usługi MSS mają na rynku unikalną gwarancję skuteczności ochrony: warunki

zdefiniowane w Service Level Agreement (SLA) przewidują rekompensaty pieniężne za ataki, które przełamały ochronę. W przypadku najwyższego poziomu SLA za każdy udany atak na zasoby klienta IBM zwraca kwotę 50 tys. USD jeśli ten atak znajduje się na prowadzonej przez X Force liście publicznie znanych ataków. Dzięki takiemu zobowiązaniu klienci mają pewność, iż dostawca usług MSS jest żywotnie zainteresowany ochroną ich infrastruktury.

Wsparcie X-Force – usługi MSS i konstrukcja ich infrastruktury technicznej bazuje na wiedzy i doświadczeniu X-Force. Ten potencjał został wykorzystany do stworzenia centrum świadczenia usług IBM MSS i jego wewnętrznych procesów, skonstruowania algorytmów automatycznego wykrywania zagrożeń oraz technik monitorowania.

Konsola wirtualnego centrum zarządzania (portal Virtual Security Operations Center - VSOC) – klient ma bezpośredni dostęp do wszystkich danych dotyczących procesu zarządzania bezpieczeństwem swojej infrastruktury oraz różnorodnych raportów charakteryzujących problemy bezpieczeństwa specyficzne dla niego. Korzystając z portalu VSOC klient ma pełną kontrolę na procesem zintegrowanego zarządzania bezpieczeństwem jego zasobów.

Zarządzanie urządzeniami różnych dostawców – Do realizacji usług IBM MSS po stronie klienta mogą być użyte urządzenia i oprogramowanie różnych producentów.

Więcej informacji

Aby dowiedzieć się więcej o oferowanych przez IBM usługach zdalnego zarządzania bezpieczeństwem infrastruktury IT skontaktuj się z zespołem IBM ISS (iss@pl.ibm.com) lub odwiedź stronę internetową:

ibm.com/services/us/iss

© Copyright IBM Corporation 2009

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

Strona główna IBM znajduje się pod adresem: **ibm.com/pl**

Wydrukowano w Polsce
Wszelkie prawa zastrzeżone.

IBM i logo IBM są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach. Proventia i X-Force są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Internet Security Systems, Inc. w Stanach Zjednoczonych i/lub innych krajach. Internet Security Systems, Inc. jest w pełni zależną filią International Business Machines Corporation.

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.