

Proaktywna identyfikacja słabych punktów zabezpieczeń sieci przy użyciu oprogramowania IBM Internet Scanner

Pierwszym krokiem do skutecznego zabezpieczenia sieci jest jej poznanie

Oprogramowanie IBM Internet Scanner stanowi solidny fundament bezpieczeństwa sieci. Umożliwia szybkie rozpoznanie i ocenę słabych punktów zabezpieczeń w systemach podłączonych do sieci, m.in. w serwerach, stacjach roboczych i urządzeniach infrastrukturalnych. Internet Scanner podnosi poziom bezpieczeństwa i pozwala uzyskać wymierne oszczędności, ponieważ automatycznie wykrywa zasoby sieciowe, rozpoznaje słabe punkty zabezpieczeń i luki w systemach operacyjnych oraz aplikacjach, a następnie ustala priorytety instalowania aktualizacji i działań zabezpieczających.

Internet Scanner sonduje systemy operacyjne, routery/przełączniki, serwery poczty, serwery WWW, firewalle i aplikacje, identyfikując ich słabe punkty, które dzięki temu mogą zostać zabezpieczone zanim hakerzy uzyskają dostęp do systemów i przejmą nad nimi kontrolę. Wyniki skanowania są prezentowane zarówno na ekranie, jak i w raportach, co umożliwia pracownikom działu informatycznego natychmiastowe reagowanie na newralgiczne luki.

Aplikacja Internet Scanner może zostać zintegrowana z systemem IBM Proventia Management SiteProtector (SiteProtector). Narzędzie to pozwala na zarządzanie rozpoznawaniem słabych punktów i innymi funkcjami zabezpieczającymi z jednej centralnej konsoli.

Dlaczego rozpoznawanie słabych punktów jest tak ważne?

Ponieważ zagrożenia są coraz liczniejsze i bardziej złożone, a straty powodowane kradzieżą informacji – ogromne.

Coraz większy stopień złożoności sieci w przedsiębiorstwach wiąże się z coraz większym narażeniem na ataki. Większość firm stosuje "reaktywne" środki bezpieczeństwa, takie jak firewalle i programy antywirusowe, które jednak z reguły chronią tylko przed znanymi

zagrożeniami. Jeśli przestępca odkryje i wykorzysta słabe punkty, o których nie wie personel firmy ani dostawcy stosowanych w niej rozwiązań zabezpieczających, może wyrządzić firmie wiele szkód, takich jak:

- **Spowodowanie niedostępności (odmowa usługi) – na przykład brak dostępu do serwera WWW lub poczty bądź awarię systemu wprowadzania zamówień;**
- **Pogorszenie wizerunku firmy – na przykład gdy użytkownicy bez odpowiednich uprawnień zmodyfikują treść serwisu WWW lub wyślą z jej kont niestosowne wiadomości e-mail;**
- **Ujawnienie poufnych informacji – na przykład utrata danych klientów lub kradzież bądź publikacja tajemnic handlowych;**
- **Modyfikacja treści serwisu www lub wysłania z kont firmowych niestosownych wiadomości e-mail przez użytkowników bez odpowiednich uprawnień.**

Wszystkie te szkody wiążą się z przestojami, utratą danych, potencjalną utratą wiarygodności oraz kosztami dla przedsiębiorstwa. Skanowanie przy użyciu narzędzia Internet Scanner pomaga ograniczyć ryzyko wystąpienia takich szkód, ponieważ umożliwia wykrywanie słabych punktów zabezpieczeń sieci i ich wyeliminowanie lub objęcie ochroną zanim nastąpi ewentualny atak.

Jak działa oprogramowanie Internet Scanner?

Rozpoznanie i ocena słabych punktów

Rzetelnie prowadzony proces zarządzania zabezpieczeniami rozpoczyna się od identyfikacji zasobów. Internet Scanner identyfikuje wszystkie urządzenia, usługi i aplikacje działające w sieci. Aplikacja Internet Scanner praktycznie nie narzuca żadnych ograniczeń co do liczby wykrywanych zasobów, a zatem jest przystosowana do obsługi rozwijających się środowisk informatycznych.

Strategie domyślne i wspólne opcje edytora strategii są gotowe do użycia natychmiast po zainstalowaniu

oprogramowania Internet Scanner. Internet Scanner efektywnie i precyzyjnie wykrywa usługi, aplikacje lub fragmenty kodu narażone na atak. Rozpoznaje także błędy w konfiguracji, które mogłyby doprowadzić do naruszenia zabezpieczeń. Wreszcie, program przeprowadza nieinwazyjne testy w celu przeanalizowania potencjalnych skutków prawdziwego ataku.

Raporty o słabych punktach

Internet Scanner generuje logiczne, łatwe do zrozumienia raporty zawierające szczegółowe informacje techniczne, operacyjne oraz dotyczące zarządzania. Każdy z raportów zawiera instrukcje działań naprawczych i adresy, z których można pobrać aktualizację zabezpieczeń i przydatne informacje.

Badania w dziedzinie zabezpieczeń

Klienci korzystający z oprogramowania Internet Scanner mają dostęp do najnowszych rozwiązań IBM w dziedzinie rozpoznawania i oceny słabych punktów zabezpieczeń. Renomowany zespół specjalistów X-Force, powołany przez IBM Internet Security Systems, wykrywa, bada i testuje słabe punkty oprogramowania. Internet Scanner pobiera aktualizacje z informacjami o najnowszych zagrożeniach, dzięki czemu jest w stanie wykryć luki w systemach użytkownika niemal od razu po ich ujawnieniu.

Dlaczego warto wybrać oprogramowanie Internet Scanner oferowane przez IBM ISS?

IBM Internet Security Systems (ISS) opracował pierwszą wersję skanera sieci ponad dziesięć lat temu. Jest to zatem stabilny, skuteczny i sprawdzony produkt. Ponieważ oprogramowanie Internet Scanner jest przystosowane do zarządzania scentralizowanego, firma może sprawować ścisły nadzór nad całym swoim środowiskiem zabezpieczeń. Rozwiązanie takie ułatwi również spełnienie wymagań formalnych, np. gdy firma musi przejść audyt bezpieczeństwa systemów informatycznych. Oprogramowanie

Internet Scanner działa jako produkt autonomiczny. Jednak w razie potrzeby można je bezproblemowo zintegrować z systemem SiteProtector oraz innymi produktami IBM ISS i centralnie zarządzać na przykład wieloma skanerami zainstalowanymi w placówkach rozszanych po świecie, a tym samym zoptymalizować procesy ochrony.

Platforma ochrony IBM

Oprogramowanie Internet Scanner stanowi integralny składnik platformy ochrony IBM, która jest centralnie zarządzanym rozwiązaniem proaktywnie chroniącym systemy informatyczne. Platforma ochrony IBM realizuje czteroczęściowy proces, który umożliwia:

- 1) *Ocenę zagrożeń;*
- 2) *Ustalenie priorytetów instalacji aktualizacji oraz działań ochronnych zmierzających do natychmiastowego ograniczenia ryzyka;*
- 3) *Nieustanną ochronę wszystkich warstw sieci;*
- 4) *Formalne wykazanie ograniczenia ryzyka i zgodności ze standardami bezpieczeństwa.*

Zapraszamy do bliższego zapoznania się z możliwościami oprogramowania Internet Scanner. Firmom spełniającym określone warunki IBM ISS proponuje skorzystanie z 30-dniowego okresu próbnego. Aby umówić się na prezentację prowadzoną w siedzibie klienta, należy wysłać wiadomość na adres: iss@pl.ibm.com.

Więcej informacji pod adresem:

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

Strona główna IBM Polska znajduje się pod adresem:

ibm.com/pl

IBM, logo IBM, ibm.com, Proventia, SiteProtector i X-Force są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Nazwy innych produktów, przedsiębiorstw i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Zawarte w niniejszym dokumencie odniesienia do produktów lub usług firmy IBM nie oznaczają, że IBM zamierza udostępnić je we wszystkich krajach.

Wszystkie dane na temat wydajności zawarte w niniejszej publikacji uzyskano w konkretnym środowisku operacyjnym w warunkach opisanych powyżej i przedstawionych na ilustracji. Wydajność uzyskiwana w innych środowiskach operacyjnych może być inna, a klienci powinni przeprowadzić swoje własne testy.

Wyprodukowano w Polsce

© Copyright IBM Corporation 2007
Wszelkie prawa zastrzeżone.