

Упреждающий поиск уязвимостей в системе безопасности корпоративной вычислительной сети с помощью IBM Internet Scanner

Для обеспечения безопасности сети необходимо хорошо знать ее инфраструктуру

Программное обеспечение IBM Internet Scanner – надежное решение для обеспечения безопасности сети. Это средство позволяет оценивать уязвимости сетевых систем, включая серверы, рабочие станции и устройства сетевой инфраструктуры. Internet Scanner повышает безопасность и позволяет экономить время и деньги благодаря тому, что может обнаруживать сетевые ресурсы, выявлять угрозы безопасности и уязвимые места операционных систем и приложений и определять приоритеты при установке обновлений и проведении других мероприятий по защите сети.

Internet Scanner анализирует операционные системы, маршрутизаторы и коммутаторы, почтовые серверы, Web-серверы, брандмауэры и приложения, определяя их уязвимости и позволяя принять меры до того, как злоумышленники смогут получить доступ к этим системам и перехватить управление ими. Результаты сканирования отображаются на мониторе компьютера и выводятся в виде отчетов, что позволяет специалистам в области ИТ быстро принимать меры для устранения критических уязвимостей.

Приложение Internet Scanner можно также интегрировать в систему IBM Proventia Management SiteProtector (SiteProtector), предназначенную для управления уязвимостями и выполнения других задач по обеспечению безопасности с помощью одной консоли.

Важность проведения оценки уязвимостей

Число угроз безопасности постоянно растет, и они становятся все более изощренными - а любая кража информации ведет к гигантским потерям.

По мере усложнения сетей предприятия возрастает риск уязвимости ее компонентов для различных атак. Большинство компаний принимают ответные меры по обеспечению безопасности, например устанавливают брандмауэры и антивирусное ПО. Эти меры, в основном, помогают лишь против известных угроз. Если злоумышленник обнаружит уязвимость, неизвестную специалистам компании и поставщикам технических решений, и воспользуется ей, последствия могут оказаться катастрофическими.

- *Снижение доступности (отказ в обслуживании) — например, Web-сервер или почтовый сервер станет недоступен или система регистрации заказов прекратит работу.*
- *Нарушение целостности - например, возможность несанкционированного доступа может позволить пользователю изменить внешний вид Web-сайта или перехватить электронную почту.*
- *Нарушение конфиденциальности - например, потеря данных о заказчиках, кража или публикация конфиденциальной информации.*

Все это приведет к простоям, потере данных, потенциальному ущербу для репутации и дополнительным затратам для бизнеса. Internet Scanner помогает уменьшить подобные риски, обнаруживая уязвимости в сети и позволяя принять меры по защите потенциальных точек проникновения в нее до проведения атаки.

Принцип работы программного обеспечения Internet Scanner

Оценка уязвимостей

Первый этап процесса управления безопасностью – это идентификация ресурсов. Программное обеспечение Internet Scanner идентифицирует все устройства, службы и приложения, работающие в сети, и может обнаружить практически неограниченное количество устройств, что позволяет масштабировать его по мере развития компании.

Стандартные политики программного обеспечения Internet Scanner и удобный редактор политик позволяют сократить время, необходимое для первоначальной настройки системы. После этого Internet Scanner точно и эффективно выявляет службы, приложения или программный код, которые могут быть подвержены атаке. Система также обнаруживает неправильные параметры настройки, которые могут стать причиной компрометации сети. Наконец, система проводит тесты, не нарушающие безопасность системы, чтобы проанализировать потенциальные результаты возможной атаки.

Отчеты об уязвимостях

Программное обеспечение Internet Scanner создает логичные, простые для понимания отчеты, в которых представлена подробная техническая, оперативная и управленческая информация. Каждый отчет содержит рекомендации по внесению исправлений и ссылки на Web-сайты поставщиков пакетов обновления, содержащие полезную информацию.

Исследование безопасности

Заказчики, использующие ПО Internet Scanner, получают в свое распоряжение самые передовые решения IBM для оценки уязвимостей. Всемирно известное подразделение IBM Internet Security Systems X-Force, занимающееся исследованием безопасности, постоянно обнаруживает, исследует и тестирует различные уязвимости программного обеспечения. При обнаружении новых угроз происходит своевременное обновление программного обеспечения Internet Scanner, что позволяет вовремя обнаруживать новые уязвимости в системе безопасности.

Преимущества использования программного обеспечения Internet Scanner, разработанного подразделением IBM ISS

Подразделение IBM Internet Security Systems (ISS) занимается разработкой этого программного обеспечения уже более десяти лет. Это надежный и точный продукт, прошедший проверку временем. Программным обеспечением Internet Scanner можно управлять централизованно, что позволяет получить более жесткий контроль над сетью и средой безопасности и обеспечить соответствие самым строгим требованиям к безопасности сети, которые предъявляются регулирующими органами. Программное обеспечение Internet Scanner может использоваться как самостоятельный продукт. Помимо этого оно без труда интегрируется в систему SiteProtector и другие продукты IBM ISS, что позволяет оптимизировать защиту и централизованно управлять удаленной установкой сканеров.

Платформа безопасности IBM

Программное обеспечение Internet Scanner является неотъемлемой частью платформы IBM, обеспечивающей превентивную защиту данных в составе единого решения по обеспечению безопасности с возможностью централизованного управления. Процесс обеспечения безопасности, реализуемый с помощью платформы IBM, состоит из четырех этапов и помогает предприятиям решать следующие задачи:

- 1) Оценка рисков безопасности предприятия в целом.*
- 2) Определение приоритетов при установке обновлений и проведении мероприятий по защите для ускорения снижения уровня рисков.*
- 3) Непрерывное обеспечение безопасности всех уровней сети.*
- 4) Демонстрация снижения рисков и соответствия заданным требованиям.*

Узнайте, как программное обеспечение Internet Scanner поможет защитить ваш бизнес от интернет-угроз. Узнайте, может ли ваша компания получить 30-дневную пробную версию. Для демонстрации системы на месте обратитесь в ближайшее отделение IBM Internet Security Systems. Чтобы узнать адреса отделений и получить дополнительную информацию, посетите сайт:

ibm.com/services/us/iss



IBM EE/A

123 317 Москва, Краснопресненская наб. 18
тел. 775 8800
факс 258-6347

Адрес домашней страницы IBM:

ibm.com

IBM, логотип IBM, ibm.com, Proventia, SiteProtector и X-Force - товарные знаки International Business Machines Corporation в США и/или других странах.

Другие названия компаний, продуктов и услуг могут являться товарными знаками или знаками обслуживания соответствующих компаний.

В данной брошюре могут содержаться ссылки или указания на продукты и услуги IBM, которые компания IBM не планирует предоставлять в некоторых странах.

Все результаты, представленные в данной статье, получены в определенной операционной среде и при указанных выше условиях и приведены только в демонстрационных целях. Результаты, полученные при других условиях, могут отличаться от заявленных. Заказчикам рекомендуется проводить собственное тестирование.

Произведено в Соединенных Штатах Америки
04-07

© Copyright IBM Corporation 2007
Все права защищены.