УДК 004.621:681.14

В.А. Хорошко,
А.Н. Чернишев

АНАЛИЗ РИСКОВ В ЗАДАЧАХ МОНИТОРИНГА БЕЗОПАСНОСТИ

В статье изложены современные подходы и средства создания эффективных систем мониторинга безопасности информационно-вычислительных систем и сетей. Предложена методика анализа рисков безопасности с учетом ценности защищаемой информации. На основе этой методики формируется оценка уровня безопасности в той или иной модели защиты.

Ключевые слова: *мониторинг безопасности, методика анализа рисков, оценка уровня безопасности.*

У статті наведено сучасні підходи та засоби створення ефективних систем моніторингу безпеки інформаційно-обчислювальних систем та мереж. Запропоновано методику аналізу ризиків безпеки з урахуванням цінності інформації, що захищається. На основі цієї методики формується оцінка рівня безпеки в тій чи іншій моделі захисту.

Ключові слова: *моніторинг безпеки, методика аналізу ризиків, оцінка рівня безпеки.*

Modern approaches and means of the creation of effective monitoring systems of the safety of information systems and networks are resulted. The technique of the analysis of the safety risks, taking into account the value of the protected information is offered. On the basis of this technique an estimation of the level of safety in this or that model of a protection is formed.

Keywords: *safety monitoring, technique of the analysis of risks, estimation of the level of safety.*

При построении сетей любого назначения и включения в них механизмов безопасности возникает необходимость мониторинга соответствия используемых механизмов защиты возложенным на них задачам реализации наличия безопасности по отношению к ценности хранимой и отрабатываемой информации.

В последние годы информационные потоки, обрабатываемые в информационно-вычислительных системах, многократно возросли, возникли технологии “клиент–сервис” и более общая технология “Internen/Intranet”, увеличилась роль дискретного управления доступом к информации с учетом факторов риска несанкционированного доступа к ней и возможностью ее потери или модификации.

Хотя в каждой системе существует своя уникальная иерархия рисков, во многих случаях большинство из них ассоциируется с работой приложений, сетевыми сервисами или с сервисами операционной системы. В первом случае отсутствуют универсальные средства поддержки мониторинга безопасности. В двух других случаях, ввиду универсальности большинства применяемых операционных

систем и сетевых протоколов, возможно использовать средства поиска наиболее широко известных уязвимых мест [1].

Такой анализ оказывается весьма эффективным средством мониторинга безопасности информационных систем.

В общем случае, построение систем мониторинга, выявляющих атаки на информацию (Intrusion Detection System – IDS), может осуществляться с использованием одной из двух технологий [1]:

– обнаружение злоупотреблений (Misuse Detection – MD);

– обнаружение аномалий (Anomaly Detection – AD).

Первый класс системы мониторинга MD-IDS сравним с антивирусными системами, подключенными к компьютерной сети. Система мониторинга MD-IDS содержит набор сигнатур, описывающих типы соединений и трафиков, которые указывают на то, что осуществляется компьютерная атака на сеть или систему.

Второй класс систем мониторинга AD-IDS использует наборы моделей "нормального" сетевого трафика, обновляемые с течением времени. Трафики, не соответствующие "эталонным моделям" отличаются как аномальные и исследуются средствами службы безопасности сети или системы.

Использование второй технологии AD-IDS получает все большее распространение, в частности, разработано более 55 таких подсистем. Большинство подсистем мониторинга ориентированы на одну операционную систему, как правило, UNIX, другие настраиваются на конкретную архитектуру сети и операционную систему (Satan), а третьи предназначены для обнаружения конкретного типа атак (Crack).

Помимо вышеперечисленных, в настоящее время еще целый ряд механизмов и средств мониторинга безопасности в информационно-вычислительных системах доведены до практических разработок.

Большинство распространенных операционных систем декларируют наличие достаточно развитых средств защиты информационных ресурсов. Как минимум, это механизмы аутентификации/авторизации, разграничения доступа, мониторинга и аудита, криптографических компонентов. Даже если реализация этих механизмов достаточна с точки зрения принятой политики безопасности, необходимо учитывать еще два множества рисков: риски, связанные с неправильной конфигурацией сети или системы, и риски, возникающие вследствие ошибок в программном обеспечении [2].

Рекомендации по второй группе рисков в большей степени зависят от политики, проводимой производителем операционной системы: в какой мере система является открытой, насколько для производителя допустимо признание наличия ошибок в своем программном обеспечении, какова его оперативность при их направлении.

Для проверки корректности системных установок (или их неизменности с момента последней проверки) существуют программные продукты класса "сканер безопасности системы". Эти продукты на сегодняшний день используются в большинстве операционных систем. К их числу относятся также такие продукты, как ASET (для операционной системы Solaris), KSA (для Net Ware и NT), SSS (System Security Scaner для Unix).

Ввиду того, что именно сетевые сервисы во многих случаях служат объектами атак на распределенные информационные системы, ставится задача автоматизированной проверки сети на уязвимость со стороны известных атак. Уязвимости, заложенные в реализации сетевых сервисов протокола TCP/IP,

достаточно хорошо проанализированы. Первым продуктом, выполняющим функцию оценки уязвимости сетевых сервисов, был пакет программ Satan. В состав пакета включены 20 проверок уязвимости сетевых сервисов. Если требования к системе включают периодические проверки по наиболее полному списку уязвимостей, то необходимо использовать более совершенные средства сканирования уязвимости.

Задача автоматического выявления несанкционированных действий и реакции на них логически связана с задачей автоматического диагностирования. Одним из средств, реализующим такие действия на уровне сетевых сервисов, является Real Secure.

Инструментальное средство Real Secure предназначено для административного управления большими объемами сетевой информации. Оно может быть использовано как для простой регистрации происходящих событий, так и для организации комплекса активных защитных мер, дополняющего функции межсетевого экрана. Отличительная особенность Real Secure состоит в том, что он создан для работы в сетях крупных организаций и способен одновременно отслеживать множество нарушающих безопасность событий в непрерывном режиме работы. Real Secure включает в себя две программные подсистемы: механизм фильтрации, осуществляющий наблюдение и активное управление сетевыми событиями, и графический пользовательский интерфейс при помощи которого пользователь получает информацию о текущих событиях, может управлять ими в реальном масштабе времени, а также устанавливать и изменять рабочую конфигурацию пакетов.

В целом, для реализации мониторинга безопасности в существующих информационно-вычислительных сетях требуется активировать средства верификации защиты в тех частях сети, с которыми связаны наибольшие риски для информационных ресурсов [3]. В настоящее время при разработке средств защиты и мониторинга безопасности выделяют три основных вида угроз: угрозы нарушения конфиденциальности обрабатываемой информации, угрозы нарушения целостности обрабатываемой информации и угрозы нарушения работоспособности сети и системы.

Оптимальным является выбор таких методов и средств защиты информационно-вычислительных систем и сетей, которые обеспечили бы наименьший риск реализации атаки в каждом конкретном случае. Для этого необходимо выполнить анализ факторов риска нарушения системы защиты с последующей оценкой общей защищенности сети и выявления ее слабых звеньев. При разработке средств мониторинга безопасности одним из ключевых вопросов является методика оценки надежности (живучести) и защищенности контролируемой системы. Общим недостатком существующих на данный момент методик оценки надежности (живучести) и защищенности сетей является субъективный характер оценки рисков возникновения угроз и атак различного рода [4].

В общем случае, защищенным от несанкционированного доступа объектом является информация. В свою очередь, ее ценность, т.е. реальная стоимость или величина убытков в случае ее уничтожения или утери конфиденциальности, изменяется в зависимости от вида информации с течением времени.

В соответствии с этим предполагается следующая классификация информации в зависимости от динамики изменения ее ценности во времени:

1) ценность информации стационарна во времени;

2) ценность информации постоянно увеличивается;
3) ценность информации постоянно уменьшается;
4) ценность информации имеет верхний экстремум;
5) ценность информации имеет нижний экстремум.

Предлагаются подходы к оценке надежности (живучести) и защищенности сетей с учетом возможных рисков возникающих угроз безопасности и ценности информации. При этом последовательно реализуется четыре подзадачи:

– выделение факторов риска и оценка их весомости при нарушении системы защиты с учетом динамики изменения ценности информации;

– построение общей модели функционирования сети в условиях действия факторов рисков;

– ранжирование по уровню опасности слабых звеньев сети;

– определение уровня защищенности сети.

В общем случае можно считать, что сеть состоит из узлов, соединенных определенной средой передачи данных, причем как для узлов, так и для среды передачи существуют каналы для осуществления несанкционированного доступа [3, 4, 5]. Вероятность осуществления несанкционированного доступа по определенному каналу будем считать риском, а канал, по которому несанкционированный доступ может быть осуществлен, будем называть фактором риска.

Пусть i-фактор риска из множества N рисков. Пусть $A_i(i=\overline{1,N})$ событие, приводящее к осуществлению несанкционированного доступа, и P_i вероятность осуществления события A_i, обусловленного фактором риска i. В общем случае будем считать, что события из множества A независимы.

Вероятности P_i разделяем на три вида в зависимости от методики их определения:

– стационарные (есть однозначно определенная методика их расчета);

– нестационарные (закономерность неоднозначная, используются экспертные оценки, статистические методы);

– трудно определяемые (вероятность того, что события, приводящие к осуществлению угрозы, будет обусловлено неучтенным фактором риска).

Если рассматривать атаку на сеть как повторяющееся воздействие (пуассоновский поток), то в общем случае можно записать.

$$P_i = e^{-\frac{\lambda_i}{\mu_i}} \frac{(\lambda_i / \mu_i)^{x_i}}{x_i!}, \qquad (1)$$

где P_i – вероятность того, что атака на сеть по i-му каналу приведет к несанкционированному доступу X раз;

λ_i – интенсивность поступления воздействия по i-му каналу;

μ_i – интенсивность обслуживания данных воздействий в сети.

В обобщенной модели рассмотрим частный случай, когда $x_i=1$, поскольку момент первой удачно реализованной попытки несанкционированного доступа наиболее важен. Кроме того, после успешной попытки несанкционированного доступа следует ожидать увеличения значения μ_i как реакции со стороны системы и увеличения λ_i как реакции атакующей стороны на успешную попытку, что

позволяет считать входной поток воздействий пуассоновским лишь с определенной степенью приближения.

Тогда при $x_i=1$ имеем

$$P_i = e^{-\frac{\lambda_i}{\mu_i}} \lambda_i / \mu_i, \qquad (2)$$

А распределение плотности вероятностей реализации несанкционированных действий по i-му каналу, как

$$P_i(t_i) = e^{-\frac{t^* \lambda_i}{\mu_i}} \lambda_i / \mu_i, \qquad (3)$$

В этом случае величина λ_i пребывает в функциональной зависимости от ценности информации, а μ_i представляет собой меру защищенности сети по i-му каналу, и при $\mu_i \to \infty$ можно считать, что канал полностью закрыт от попыток несанкционированного доступа.

После проведения оценки P_i для ряда наиболее характерных факторов риска выполняется общая оценка безопасности сети.

В предлагаемом подходе, в отличие от существующих методик, учитываются изменения ценности информации с течением времени и, соответственно, вероятности осуществления несанкционированного доступа; также атаки представляются как повторяющиеся воздействия, что позволяет использовать математический аппарат теории вероятностей. Преимуществом предложенной методики является комплексное определение степени защиты информационно-вычислительных систем и сетей, что обеспечивает оптимальный уровень их безопасности, исходя из разнородных критериев. Механизм на основе предложенной методики реализуется в виде определенной подсистемы в комплексе мониторинга безопасности систем и сетей.

Специализированные системы мониторинга и тестирования защищенности сетей должны присутствовать во всех сетях с высокими требованиями к безопасности информационных ресурсов, сетях, работающих в условиях высоких рисков или являющихся вероятным объектом атаки.

Хотя количество программно-технических средств данного типа относительно невелико, необходимо подбирать эффективное решение в соответствии с корпоративной политикой безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *B. Mukherjce, L.T. Heberlein,* k.N / levitt. Network Intrusion Detection // IEEE Network, May/June. 2004. – p.p. 26–41.

2. *Ленков С.В.* Методы и средства защиты информации: в 2-х т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008.

3. *F. Venema* TCP Wrapper Network Monitoring, Acces Control and Booby Traps // USENIX Proceedings, UNIX Security Symposium X, September, 2000.

4. *Мороз Е.С.* Методы противодействия сестевым стакам / Е.С. Мороз, В.А. Хорошко, Е.Е. Смычков // Збірник наукових праць СНУЯЕ та П, Севастополь, 2007. – т. 18 (№ 5). – С. 180–187.

5. *Грищук Р.В.* Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень / Р.В. Грищук. – Житомир : Рута, 2010. – 280 с.

Отримано 10.02.2012