УДК 681.3.06:519.248.681

ПОДХОД К ВЫРАБОТКЕ РЕШЕНИЙ ПРИ РЕАГИРОВАНИИ НА АНОМАЛЬНОЕ СОСТОЯНИЕ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

А.В. Снегуров
Кандидат технических наук, доцент
Кафедра телекоммуникационных систем*
Контактный тел.: 8 (057) 702-10-67
Email: arksn@rambler.ru

В.О. Солод
Контактный тел.: 8 (093) 720-47-15
Email: Fe.male@mail.ru
*Харьковский национальный университет радиоэлектроники
Пр. Ленина, 14, г. Харьков, 61166

В статті запропоновано підхід до відпрацювання рішення на вибір захисних заходів при виявленні аномального стану телекомунікаційної мережі з використанням нечітких бінарних відношень

Ключові слова: телекомунікаційна мережа, аномальний стан, комп'ютерна атака

В статье предлагается подход к выработке решения на выбор защитных мероприятий при обнаружении аномального состояния телекоммуникационной сети с использованием нечетких бинарных отношений

Ключевые слова: телекоммуникационная сеть, аномальное состояние, компьютерная атака

Methods to the solution of selecting protective measures to detect an anomalous state of a telecommunication network by using fuzzy binary relations are proposed.

Key words: telecommunication network, anomalous state, cyber attack

Постановка проблемы

Обеспечение безопасности телекоммуникационных сетей и систем является в настоящее время одной из наиболее острых проблем. Ведущие эксперты по информационной безопасности отмечают резко возросшую опасность кибератак на государственные и корпоративные информационные системы и сети [1]. Противоборство в киберпространстве приобрело таких масштабов, что любая организация, эксплуатирующая телекоммуникационные сети, должна использовать средства защиты от компьютерных атак.

В настоящее время разрабатываются и уже успешно реализованы различные системы обнаружения вторжений (Intrusion Detection System, IDS), которые в дополнение к межсетевым экранам служат механизмами мониторинга и наблюдения подозрительной активности в сети. Положительной стороной системы обнаружения вторжений, построенной по методу аномалий, является возможность обнаружения вторжения, сигнатуры которого не известны. Это позволяет обнаруживать ранее не известные компьютерные атаки, что особенно актуально на современном этапе. Однако существенным недостатком таких систем является сложность описания параметров нормального и ненормального функционирования сети. Данные системы имеют большие вероятности пропуска атак и выдачи ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности. Данные недостатки могут существенно уменьшить эффективность работы IDS. Так, большое количество ложных сигналов может привести к тому, что администратор безопасности прекращает реагировать на сообщения системы обнаружения вторжений.

В этих условиях актуальной задачей является разработка механизма принятия решения системой безопасности при выходе параметров сети за пределы нормального функционирования. Однако проблема заключается в том, что функционирование сети зависит от множества факторов. К таким факторам могут относиться внешние и внутренние условия функционирования телекоммуникационной сети, задачи, решаемые организацией, эксплуатирующей телекоммуникационную сеть и т.д. В качестве примера можно привести появление внешнего воздействия

на организацию (например, постановка организации новой сложной задачи, которая выводит организацию из ее нормального «повседневного» состояния и т.д.). Это может привести к изменению активности пользователей сети. В этих условиях система безопасности начнет давать сбои, что негативно скажется как на обеспечении безопасности организации, так и эффективности выполнения организацией своих задач.

Вопросам защиты телекоммуникационных сетей от вторжений посвящено большое количество работ [2 – 5]. В то же время, недостаточно разработанными являются методы принятия решения при реагировании на аномальные состояния в сложных условиях функционирования телекоммуникационной сети.

Цель статьи – рассмотреть подход к принятию решения, позволяющий выработать эффективное управленческое решение при обнаружении аномального состояния телекоммуникационной сети.

Основной материал исследования

Пусть имеем множество признаков $Y=\{y_1,y_2,...,y_m\}$, на основании которых определяется состояние сети. В качестве таких признаков могут быть, например, количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и т.д.

Пусть имеем множество атак $A=\{a_1,a_2,...,a_Q\}$. Для каждой атаки введем нечеткую степень ее опасности для телекоммуникационной сети d_q, $d_q=[0,1]$, $q=\overline{1,Q}$. Данный показатель задается с участием руководства организации, эксплуатирующей телекоммуникационную сеть, и учитывает степень вреда организации от данного вида атаки. Так, например, для одной организации будет критично хищение конфиденциальной информации, а для другой атаки типа DDos, приводящие к отказу в обслуживании.

Пусть имеется множество условий функционирования сети (зависящая от условий функционирования организации, эксплуатирующей сеть) $U=\{u_1,u_2,...,u_G\}$. Такими условиями могут быть: дневное время – работа; дневное время – перерыв; ночное время; решение организацией определенной задачи и т.д. При задании условий функционирования сети необходимо учитывать критические моменты «жизни» организации. Так решение организацией важной задачи может привести к тому, что во внерабочее время интенсивность работы сети будет намного больше, чем в «обыкновенные» периоды.

Также пусть имеется множества состояний сети $S_g=\{s_1,s_2,...,s_N\}$, $g=\overline{1,G}$, при разных условиях ее функционирования. Так, одно состояние сети для рабочего времени может быть нормальным, а для нерабочего времени – аномальным.

Пусть имеется множество решений системы безопасности $B=\{b_1,b_2,...,b_z\}$. Каждое из своих решений система безопасности принимает на основании мониторинга сети с использованием множеств A, U, S и правила принятия решения.

Построим матрицу R_g нечеткого бинарного отношения для каждого g условия функционирования сети:

$$R_g=\begin{vmatrix}\mu_{s_1}^{a_1}\ \mu_{s_1}^{a_2}\ ...\ \mu_{s_1}^{a_Q}\\ \mu_{s_2}^{a_1}\ \mu_{s_2}^{a_2}\ ...\ \mu_{s_2}^{a_Q}\\ ...\ ...\ ...\ ...\\ \mu_{s_N}^{a_1}\ \mu_{s_N}^{a_2}\ ...\ \mu_{s_N}^{a_Q}\end{vmatrix},$$

где $\mu_{S_n}^{a_q}, q=\overline{1,Q}, n=\overline{1,N}$, $\mu_{S_n}^{a_q}=[0,1]$, - нечеткая степень возможности возникновения S_n состояния телекоммуникационной сети при применении нападающей стороной a_q вида атаки на сеть. Данная матрица показывает, как повлияет тот или иной вид атаки на изменение параметров сети, являющимися признаками для ее мониторинга системой безопасности.

Построим также матрицу W нечеткого бинарного отношения:

$$W=\begin{vmatrix}\mu_{a_1}^{b_1}\ \mu_{a_1}^{b_2}\ ...\ \mu_{a_1}^{b_z}\\ \mu_{a_2}^{b_1}\ \mu_{a_2}^{b_2}\ ...\ \mu_{a_2}^{b_z}\\ ...\ ...\ ...\ ...\\ \mu_{a_Q}^{b_1}\ \mu_{a_Q}^{b_2}\ ...\ \mu_{a_Q}^{b_z}\end{vmatrix},$$

где $\mu_{a_q}^{b_z}, z=\overline{1,Z}, q=\overline{1,Q}$, $\mu_{a_q}^{b_z}=[0,1]$, - степень эффективности b_z – го решения системы безопасности сети от a_q вида атаки. Данные показатели задаются должностными лицами системы безопасности на основании имеющейся информации об эффективности защитных мероприятий от компьютерных атак, на основании личного опыта, а также интуитивно (если информации нет).

Из матриц R_g и W формируется матрица T_g:

$$T_g=\begin{vmatrix}\mu_{s_1}^{b_1}\ \mu_{s_1}^{b_2}\ ...\ \mu_{s_1}^{b_z}\\ \mu_{s_2}^{b_1}\ \mu_{s_2}^{b_2}\ ...\ \mu_{s_2}^{b_z}\\ ...\ ...\ ...\ ...\\ \mu_{s_N}^{b_1}\ \mu_{s_N}^{b_2}\ ...\ \mu_{s_N}^{b_z}\end{vmatrix},$$

элементы которой определяются функцией принадлежности:

$$\mu_{s_n}^{b_z}=\sum_{n=1}^{N} d_q\cdot\mu_{s_n}^{a_g}\cdot\mu_{a_q}^{b_z}\ \text{для всех}\ n=\overline{1,N}, q=\overline{1,Q}, z=\overline{1,Z}. \quad (1)$$

Данный показатель определяет эффективность выбора b_z варианта решения системой безопасности при наблюдении s_n состояния телекоммуникационной сети. В качестве таких решений может быть выбор из заданного множества средства защиты или продолжение мониторинга сети.

Выбор варианта решения системой безопасности телекоммуникационной сети может осуществляться в два этапа. На первом этапе для каждого s_n состояния сети на основании порогового значения показателя $\mu_{s_n}^{b_z}$ пор принимается решение о необходимости актив-

ных действий системы безопасности. Смысл данного этапа заключается в том, что при нормальном функционировании сети за счет показателей матрицы R_g, показатель $\mu_{s_n}^{b_z}$ не будет превышать его порогового значения $\mu_{s_n}^{b_z}$ пор. В этом случае система безопасности активных действий осуществлять не будет. Для состояний сети, при которых показатель $\mu_{s_n}^{b_z}$ превышает заданное пороговое значение («опасность атаки»), выбор варианта действий системы безопасности осуществляется на основании выражения:

$$b(s_n) = \max\left[\mu_{s_n}^{b_z}\right] . \quad (2)$$

В соответствии с выражением (2) для s_n состояния телекоммуникационной сети (являющегося «опасным») выбирается такой вариант решения системы безопасности, при котором показатель $\mu_{s_n}^{b_z}$ будет максимальным (решение будет самым эффективным).

Выводы

Данный подход к выработке решения при возникновении аномальной ситуации в телекоммуникационной сети позволяет учесть изменение условий функционирования сети, опасность атаки, эффективность защитных мероприятий от сетевых атак. Дальнейшие исследования будут направлены на практическую реализацию предлагаемого подхода.

Литература

1 Игорь Громов. США беззащитны перед стратегическими хакерскими атаками [Электронный ресурс] / Лаборатория Касперского. – Режим доступа: http://www.viruslist.com/ru/hackers/news/ - 28.04.2007 г. – Загл. с экрана.

2. Петренко С.А., Беляев А.В. Проблема обнаружения компьютерных атак в критически важных инфраструктурах / С.А. Петренко, А.В. Беляев // Защита информации. INSIDE. - 2008. - № 2. – С. 32 – 36.

3. Душкин А.В. Распознавание и оценка угроз несанкционированного воздействия на защищенные информационно-телекоммуникационные системы / А.В. Душкин // Информационные технологии. – 2008. - № 3. – С. 71 – 75.

4. Балашов П.А., Кислов Р.И., Безгузиков В.П. Оценка рисков информационной безопасности на основе нечеткой логики / П.А. Балашов, Р.И. Кислов, В.П. Безгузиков // Защита информации. Конфидент. - 2003. - № 4. - С. 56 – 59, № 5. - С. 60 – 65.

5. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко, – К.: МК-Пресс, 2006. – 320 с.

6. Нечеткие множества и теория возможностей. Последние достижения: пер. с англ./ Под ред. Р.Р. Ягера. – М.: Радио и связь, 1986. – 408 с.