И.А. Носаль

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО ВАЖНЫХ ОБЪЕКТОВ

(Санкт-Петербургский институт информатики и автоматизации РАН)

Под социально-важным объектом (далее – СВО) в данной работе будем понимать социально ответственный институт, не входящий в систему органов государственной власти и не являющийся государственным учреждением, основной целью которого является предоставление социально значимых государственных услуг и обеспечение прав граждан, прерывание работы которого может привести к нарушению стабильности в обществе и нормальных условий жизнедеятельности населения. Примеры таких организаций – Фонд социального страхования, Фонд обязательного медицинского страхования, Пенсионный фонд Российской Федерации. Все эти организации по форме образования и расходования денежных средств являются внебюджетными государственными фондами, имеют схожие цели, задачи, принципы работы, административно- управленческую структуру и являются крупнейшими операторами персональных данных.

Информационная безопасность СВО – это одно из главнейших условий надлежащего предоставления СВО качественных государственных услуг, является частью системы национальной безопасности и внутренней политики, а также влияет на безопасность личности, общества и государства. Для государства обеспечение информационной безопасности СВО – гарантия надлежащего исполнения своих функций (обязательств перед населением).

В отличие от государственной безопасности, для обеспечения информационной безопасности СВО предоставляется значительно меньше инструментов и ресурсов, однако предъявляется достаточно много требований, как со стороны государства, так и со стороны населения. Поэтому мы можем назвать информационную безопасность (ИБ) СВО системой с множеством взаимозависимых субъектов и объектов защиты, где каждый субъект может быть классифицирован исходя из задач, которые он решает с помощью СВО, а значит требований, которые он предъявляет к ИБ СВО и актуальным для него объектам защиты.

Основное отличие ИБ СВО – это частичная принадлежность к системе обеспечения государственной безопасности. Во-первых, это слияние и наследие принципов и способов ИБ, используемых при обеспечении государственной безопасности, частично надиктовываемая политика в отношении ИБ СВО, а во-вторых жесткий контроль государственных регуляторов. При этом, отсутствует представление, о том какой вообще должна быть система информационной безопасности СВО. Основным подходом, который используется при построении ИБ СВО становится выполнение требований регуляторов, что недостаточно для комплексного обеспечения информационной безопасности,

поскольку требования разрабатываются без учета особенностей организации (специализации), зачастую противоречивы, в основном охватывают узкий перечень защищаемых ресурсов и, поскольку технический прогресс вносит свои коррективы быстрей, чем регулирующий орган в законодательство, устаревают.

Требования разных регуляторов часто дублируются или вступают в противоречие друг с другом. Как следствие, это грозит нарушениями или затруднением деятельности СВО, увеличением нагрузки на персонал, усложнением документооборота, дублированием документации, мер и методов защиты. Главный недостаток этого решения – отсутствие комплексного подхода, что может привести к появлению «дыр» в системе защиты, утечкам защищаемой законом информации и нарушению непрерывности (останову) основных производственных процессов. Разработка отраслевого стандарта значительно продвинула бы развитие ИБ СВО и этот вопрос по вышеуказанным причинам требует активного участия со стороны государства и поддержки профессионального сообщества.

То, какой будет структура системы информационной безопасности организации, определяет в большей степени отношение организации к состоянию «безопасности». К примеру, для государственной безопасности отсутствие контроля над защищаемым объектом на какой угодно малый промежуток времени уже является реализованной атакой (значимым инцидентом равносильным утечке). Не требуется доказательство факта утечки, достаточно одного только подозрения в этом, т.е. бесконтрольного пребывание объекта.

Для автоматизированных систем управления технологическим процессом (АСУ ТП) важно – был ли факт нарушения производственного процесса и насколько критичны последствия (причинён ущерб только установке, зданию, заводу, концерну, региону, государству, населению). Для банковского сектора важно наличие огласки инцидента (репутация) и размер денежных потерь банка (насколько он критичен), вне зависимости от того, была ли реализована или остановлена атака (угроза). Для СВО важно – был ли нанесен в результате ущерб населению или государству (прямой или косвенный) и его размер.

Для коммерческой организации риск-менеджмент подход соответствует ценностям бизнеса – сами по себе расходы (ущерб от реализации атаки) не являются чем-то негативным, при условии, что расходы не должны превышать доходы. То есть, мы пытаемся предотвратить нанесение ущерба только тогда, когда его предотвращение стоит дешевле, чем его реализация.

Государственная безопасность оперирует другими понятиями о безопасности: тут либо ноль, либо единица – неопределенность и вероятностный подход не годится, но это для СВО очень дорогостоящий подход. В отличие от государственной безопасности, для обеспечения информационной безопасности СВО предоставляется значительно меньше инструментов и ресурсов.

У СВО отличное от вышеназванных организаций понимание «информационной безопасности». Риск-менеджмент вполне приемлем для СВО, если не брать во внимание, что здесь ущерб рассчитывается не по отношению в СВО, а по отношению к его клиентам (остановка/нарушение работы самого СВО наносит ущерб населению). Что сделать сложнее настолько, насколько сложнее определить ценность той или иной информации для каждого конкретного человека и обобщить этот показатель.

Следует отметить, что СВО очень подвержены атакам третьего поколения как находясь в положении жертвы, так и будучи задействованным в качестве третьего лица (посредника). В ситуации, когда СВО подвергается атаке третьего поколения, урон информационным ресурсам СВО может быть не на нанесен вовсе, однако репутационные риски могут быть очень велики.

Поскольку информационная безопасность СВО защищает интересы населения, все риски, в том числе и репутационные, и нанесенный ущерб мы должны рассчитываться в отношении населения, чего мы сделать не можем, а значит репутационные риски для СВО не характерны. С другой стороны, СВО являясь инструментом государственного регулирования социальной жизни страны, воспринимается населением как орган государственной власти и отношение населения к СВО имеет прямое влияет на репутацию государства и состояние национальной безопасности. В этом разрезе сохранение положительной репутации СВО очень важно в рамках внутренней безопасности государства.

Существует также дополнительное следствие - восприятие СВО населением как части государственной власти приводит к тому, что репутация государственной власти в равной степени распространяется на СВО. К примеру, если какой либо из органов понес репутационный ущерб и потерял определенный процент доверия населения, эта потеря скажется на всей системе государственной власти и СВО в том числе.

Такой специфичный подход к оценке ущерба СВО накладывает определенные ограничения при обосновании управляющих решений по обеспечению ИБ СВО.

Литература

1. Фазлутдинова Э. Сплошной мониторинг // «Я работаю в ПФР». 2013. № 4/50. С. 4

2. Бондарева Н. Владельцы ситуации // «Я работаю в ПФР». 2011. № 3/3. С. 3

3. Евдокимова А. АИС – технологическая азбука ПФР // «Я работаю в ПФР». 2012. № 10/40. С. 1-2

4. Brotby K. Information security governance. A Practical Development and Implementation Approach - Hoboken: John Wiley & Sons, Inc., 2009 – 185 s.

5. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М.: Издательский центр «Академия». 2009. 416 с.

6. Security threat modeling and analysis: a goal-oriented approach. Ebenezer A. Oladimeji, Sam Supakkul, Lawrence Chung//Режим доступа: - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10 .1.1.103.2997&rep=rep1&type=pdf

7. Миронов В. В., Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена зам.директора ФСТЭК России от 14.02.2008

9. ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007 Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий; Введ. 01.09.2007. – М.: Стандартинформ, 2006 -49с.

10. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с. // Хоффман, Л. Д. Современные методы защиты информации / Л. Д. Хоффман; под ред. В.А. Герасименко. М.: Сов. радио, 1980. — 264 с.

Р.М. Пасечник, О.И. Барсуков

ИСПОЛЬЗОВАНИЕ DNS-ЗАПРОСОВ В КАЧЕСТВЕ СРЕДЫ РЕАЛИЗАЦИИ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ

(Кубанский государственный технологический университет)

В настоящее время одной из актуальных угроз обеспечения информационной безопасности в автоматизированных системах является использование злоумышленниками скрытых каналов передачи информации в открытых компьютерных системах (в том числе в сетях связи общего пользования). Необходимо констатировать факт, что проблематике использования скрытых каналов в сетях передачи данных не уделяется необходимого внимания.

В данной статье рассматривается вопрос использования DNS-запросов в качестве среды для создания нетрадиционного (скрытого) канала передачи информации. Реализация данного способа передачи данных основывается на технологии «туннелирования» TCP/IP трафика по средству DNS-запросов, т.е. инкапсуляции TCP/IP трафика в DNS-запросы.

В настоящий момент, данный метод рассматривается мировым ИТ-сообществом только с целью получения доступа в глобальную сеть Интернет через Wi-Fi сети в обход авторизации пользователей на web-форме*.

Помимо безвредного, на первый взгляд, доступа в сеть Интернет (но уже по сути являющимся правонарушением), данной технологией могут пользоваться злоумышленники, для достижения таких целей как:

* Такой метод авторизации в основном применяется для обеспечения коммерческого доступа в сеть Интернет в аэропортах, гостиницах и др. общественных местах