работ по устранению инцидента службам сервиса ИТ-объекта, на котором произошёл инцидент; но заказ этими службами выполняется только в их рабочее время;

– уровень 5, критический (авария, disaster); при обработке такого алерта вместе с сообщением о нём на e-mail формируется заявка критического уровня важности (critical priority ticket) в систему HPSM, но устранение инцидента службами сервиса ИТ-объекта после получения заявки выполняется в любое время суток, в том числе и в выходные дни.

Для оценки действенности предлагаемой приоритизации алертов анализируется их список за ноябрь 2014 года [2].

Литература

1. NIST special publication 800-61 Revision 2. Computer security incident handling guide.

2. *Николаенко В.А., Прузан А.Н., Сечко Г.В., Таболич Т.Г.* Опыт мониторинга инцидентов информационной безопасности в облачных вычислениях // Сб. статей III межд. заоч. НПК «Информационные системы и технологии: управление и безопасность» (декабрь 2014). – Тольятти-Русе: Поволжский гос. университет сервиса в партнёрстве с Русенским университетом «Ангел Кънчев» (Болгария), 2014. С. 209–215.

ПРИМЕНЕНИЕ VPN ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ VOIP

А.А. Антонников, С.Н. Петров

В настоящее время большую популярность приобретают различные сервисы, связанные с пакетной передачей данных по IP протоколу. Одними из наиболее популярных являются сервисы IP-телефонии, определяемые общим стеком VoIP-протоколов. Применение данной технологии позволяет снизить стоимость телефонных соединений при высоком качестве сервиса. Распространение технологии VoIP оказалось сопряжено с проблемами, связанными с защитой речевой и сигнальной информации. Так как технология передачи речевого трафика является частным сегментом пакетной передачей данных по IP протоколу, система VoIP телефонии испытывает те же угрозы, присущие обычным сетям, а также спектр угроз безопасности связанный сугубо с данным сегментом.

Рост количества и разнообразия пользовательских устройств, вызвал необходимость защиты речевого трафика от каждого конечного терминала. Обеспечение безопасности в сетевой инфраструктуре реализовано при помощи сложных программно-аппаратных комплексов, которые обеспечивают безопасность различными методами на различных уровнях. Данное решение должно быть гибким, обеспечивать устойчивое шифрование, а также быть кроссплатформенным.

Одним из наиболее подходящих решений является программный продукт с открытым исходным кодом OpenVPN. OpenVPN это open source технология, обеспечивающая надёжный криптоканал связи между пользователем и сервером. OpenVPN использует для обеспечения безопасности потока данных протоколы SSL/TLS, а, следовательно, поддерживает все возможности шифрования, аутентификации и сертификации библиотеки OpenSSL. OpenVPN является достаточно сложным при установке и настройке.

В докладе рассмотрен вариант реализации сети VoIP на основе технологии OpenVPN. Для заданной структуры телефонной сети предприятия определены основные уязвимости и угрозы информационной безопасности. Предложены варианты настройки шифрования и аутентификации.

ОПТИМИЗАЦИЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ПРЕДПРИЯТИЯ

П.А. Домино, С.Н. Петров

Ограничение доступа является важным условием соблюдения такого свойства информации, как конфиденциальность. Обязательной частью управления доступом является

аутентификация, без нее нет возможности ограничить доступ пользователей к конкретным информационным ресурсами.

Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли. Этот способ аутентификации получил самое широкое распространение. Главные достоинства парольной аутентификации – простота и привычность.

Сегодня количество программных продуктов, используемых в любой компании, довольно велико. И можно с уверенностью сказать, что существует тенденция увеличения их количества, причем независимо от профиля компании.

Многие из используемых приложений требуют прохождения аутентификации, то есть указания логина и пароля пользователя. При этом с точки зрения пользователей, при использовании паролей возникают следующие проблемы: возрастает как число используемых паролей, так и их сложность, с определенной периодичностью пароли необходимо менять.

Для облегчения процесса парольной аутентификации многие пользователи прибегают к таким мерам, как использование простых паролей, использование одного пароля во множестве приложений, запись паролей на стикерах или использование в качестве пароля какого-то символа, находящегося в пределах их рабочего места (модель монитора, например). В результате этих действий уровень информационной защищенности компании значительно понижается.

В работе рассматриваются методики оптимизации системы аутентификации пользователей. Проведен обзор и анализ существующих механизмов аутентификации, рассмотрены способы оценки эффективности механизмов аутентификации, а также исследованы результаты оптимизации существующих механизмов аутентификации в корпоративной сети предприятия.

СИСТЕМА РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ ПОСРЕДСТВОМ PEER-TO-PEER СЕТИ

Е.В. Разумов

В информационном обществе главным ресурсом является информация. В данный момент большая часть информации хранится и передается в цифровом виде. При этом важным аспектом является хранение, а также передача конфиденциальной информации.

В настоящее время существует множество различных способов обеспечения безопасной пересылки данных. И наиболее распространенным из них является способ, основанный на использовании протоколов SSL [1] и его модификации TLS. Однако при этом существует ряд атак, которые применимы даже для SSL соединения. Одной из них является так называемая MITM-атака (man in the middle). Она подразумевает наличие атакующего, который способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале.

Одним из возможных методов, по средствам которого можно достичь большую устойчивость к MITM-атакам, является метод построения системы распределенной передачи данных посредством peer-to-peer сети. Основная идея, заложенная в данную систему, заключается в разбиении передаваемой информации на блоки, шифровании каждого из этих блоков и последующей передаче их через отдельный промежуточный узел. Размер блоков и их количество может быть выбрано произвольно. От этих параметров будет зависеть число участвующих в передаче узлов сети и, соответственно, скорость передачи. В передаче необходимой информации могут участвовать не все узлы, в то время как некоторые узлы могут участвовать в этом более одного раза.

Таким образом разработанная модель решает проблему перехвата сообщения целиком, так как злоумышленник не может изначально знать через какие узлы будут передаваться части сообщения, а внедриться между всему участвующими узлами сети при достаточно большом количестве этих узлов практически не представляется возможным. К тому же даже перехват