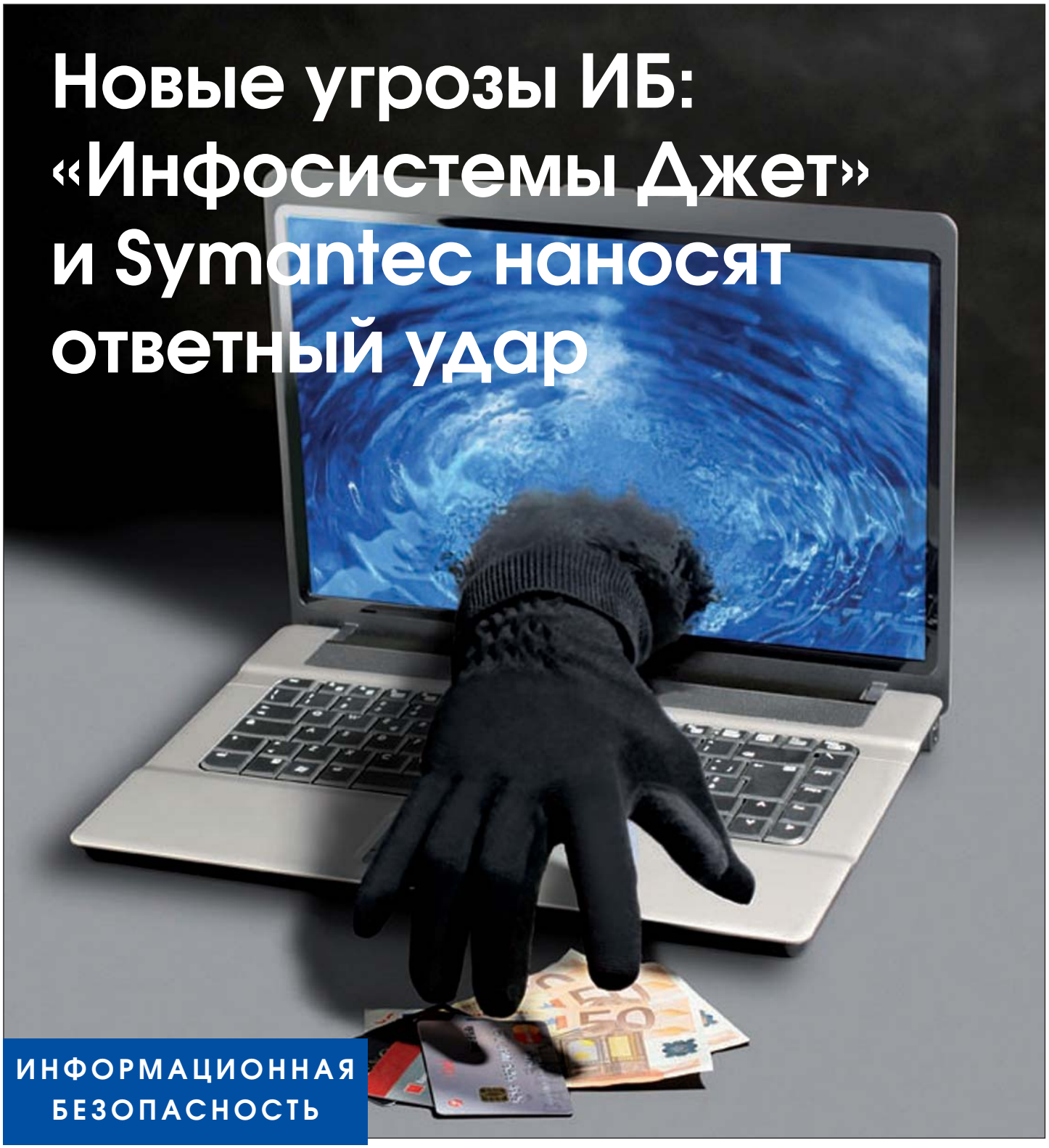
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 4 (191)/2009

Новые угрозы ИБ: «Инфосистемы Джет» и Symantec наносят ответный удар



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Новые угрозы ИБ: «Инфосистемы Джет» и Symantec наносят ответный удар

Игорь Ляпунов, Алексей Воронцов, Мария Датриева,
Центр информационной безопасности
компании «Инфосистемы Джет»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационная безопасность. Мы победили!...?

Игорь Ляпунов,
руководитель Центра информационной безопасности
компании «Инфосистемы Джет»

В нашем издании мы стараемся освещать новые или даже инновационные темы, интересные технологии и технологические решения. Но сегодня хочется посвятить несколько слов проблеме, которая стала уже традиционной — вредоносному контенту и вирусам. По сравнению с тем, как эта тема обсуждалась в научно-популярной прессе несколько лет назад, какие дискуссии разворачивались на конференциях, можно сказать, что сейчас наступил штиль — ажиотаж поутих.

Может быть мы победили? Ведь все производители средств защиты прошли очень серьезный путь в развитии и повышении зрелости своих технологий и продуктов. Каждое интегрированное сетевое средство защиты имеет в своем составе очень гибкие механизмы обнаружения атак и блокирования вредоносных активностей. А если помните, всего несколько лет назад нужно было доказывать, зачем в сети нужны средства обнаружения атак, а технологии предотвращения вторжений и активной безопасности вообще казались сказочными. Сегодня это норма. Про антивирусы, межсетевые экраны и говорить не приходится. Каждый ИТ-специалист знает, что по утрам нужно чистить зубы, на входе в сеть нужно ставить экран, а на рабочем месте — антивирус. Все? Мы не оставили злоумышленникам ни единого шанса?

Подозреваю, что ответить утвердительно будет очень сложно. Буквально недавно к нам обратились две компании с одним и тем же вопросом — некоторые рабочие стации заблокировались и просят отправить куда-то SMS, чтобы получить код разблокировки. Вылечить эту проблему, вообще говоря, не сложно. Но важен сам факт. Ведь вирусные заражения страшны в первую очередь тем, что это в некотором смысле индикатор — лакмусовая бумажка общего состояния защищенности ИС и качества системы защиты информации. Если у вас возник инцидент с вирусами, это значит, что какой-то из каналов их проникновения не закрыт, кто-то получил его по почте или принес на флэшке, это значит что антивирусные базы не обновились вовремя или пользователь смог отключить антивирус. Это значит, что у вас нет полного контроля за вашей информационной системой, процессы управления информационной безопасностью дали сбой. А это чревато.

При этом хочу отметить, что активность классических вирусов несколько снизилась, массовые эпидемии уже не так часто развиваются. Сильно возросла их целенаправленность. Вирус ради вируса уже не пишут. Их пишут исключительно ради денег. Это часть одной большой «пищевой цепочки». Участником каждой серьезной сетевой атаки, взлома системы, хищения всегда является вирус или троян. Бот-сети, украденные пароли, ключи, с которых начинается атака — дело их рук. В недавнем инциденте в одном из российских банков была осуществлена атака на систему дистанционного банковского обслуживания. Была попытка перевести деньги со счетов клиентов. При этом криптографические ключи

были украдены злоумышленниками с помощью специально разосланного по клиентам банка трояна.

Почему такое возможно в эпоху развитой безопасности и торжества защитных технологий? Типичных ошибок две.

Первая. Когда что-то делаешь, что-то строишь или от кого-то защищаешься нельзя это делать с закрытыми глазами. Только с комарами можно бороться на ощупь. Во всех остальных ситуациях вы должны контролировать достижение цели: попали — не попали, убили — не убили. Вы построили забор. Просто так к вам уже никто не проникнет. Но кто знает, может быть, воры начали через верх лазить и пора сверху колючую проволоку натягивать? Или наоборот снизу копают? Ровно тоже самое с системами безопасности. Если вы не мониторите состояние вашей системы, не отслеживаете логи, не разбираете каждый инцидент, то у вас завязаны глаза, а вокруг — грабли. Да, согласен, ежедневный анализ логов дело очень трудоемкое и рутинное. Но без него никуда. Если у вас два сервера, то заставьте себя и сделайте это. Если пять и на двух площадках, то возьмите специального человека. Если больше — начинайте думать про системы автоматизированного сбора лога и анализа событий.

Вторая. Такая же нудная. Защита рабочих мест конечных пользователей. Сам процесс не всегда приятен, пользователи всегда сложные. К ним нужно прислушиваться, оценивать, что они в состоянии выполнить, а что нет. Многократно объяснять и показывать. Если вы хотите предложить решение, которое им сильно усложнит работу — не тратьте время. Они найдут способ этого не делать. Вы всегда будете искать компромисс. Но если не построить надежной защиты конечных рабочих мест, то так и будут ваши пользователи спрашивать, а нужно ли отправлять SMS, чтобы разблокировать компьютер. Даже один компьютер, на котором не обновлен антивирус — это рассадник заразы по всей сети.

Вот этим двум проблемам и будет посвящен нынешний номер нашего издания. Мы расскажем о практических подходах к построению центров оперативного мониторинга и защите рабочих мест пользователей на примере технологий Symantec.

Компания «Инфосистемы Джет» получила статус Центра компетенции Oracle по направлению Enterprise Performance Management: Business Intelligence and Data Warehousing

Присвоение данного статуса свидетельствует о высоком профессионализме и значительном опыте специалистов компании «Инфосистемы Джет» в реализации проектов по внедрению решений Oracle Business Intelligence. Это второе технологическое направление Oracle, по которому компания открыла Центр компетенции (первый Центр компетенции был открыт по направлению Oracle Fusion Middleware: Identity and Access Management).

В него входят тестовая лаборатория и демонстрационная зона прикладных продуктов Oracle. Центр оснащен необходимым вычислительным, коммуникационным и технологическим оборудованием. В рамках подготовки специалистов для Центра компетенции 17 человек прошли обучение по продуктам Oracle, причем четверо из них по курсам Oracle Business Intelligence. Специалисты Центра компетенции обладают высокой квалификацией в области внедрения, эксплуатации и поддержки хранилищ данных и аналитических приложений.

Все это позволяет компании «Инфосистемы Джет» реализовывать проекты различного уровня сложности и наглядно демонстрировать преимущества продуктовой линейки Oracle Business Intelligence. Примером успешной реализации решения по бизнес-аналитике может являться проект в КБ «Транспортный», где для организации кросс-продаж в Oracle Siebel CRM была произведена сегментация клиентской базы с помощью Oracle Business Intelligence Enterprise Edition.

Компания «Инфосистемы Джет» провела семинар «Цели и задачи информационной безопасности в финансовых организациях в современных экономических условиях»

Лейтмотивом данного мероприятия стали изменения подходов финансовых организаций к обеспечению информационной безопасности: с одной стороны, каждая инициатива пристально рассматривается и все чаще ресурсы выделяются только в случае крайней необходимости, с другой — появились новые требования регуляторов (прежде всего ФЗ №152 «О персональных данных» и PCI DSS), которые иногда остаются единственными «двигателями» проектов по ИБ.

Специалисты компании «Инфосистемы Джет» рассказали о собственной практике и опыте внедрения средств защиты информации в финансовых организациях. Обсуждались также законодательные аспекты информационной безопасности, меры и технические способы по защите персональных данных.

На семинаре были рассмотрены причины утечки конфиденциальной информации кредитно-финансовых учреждений, а также предложены методы минимизации рисков потери данных. Данные методы основаны на реальном проектном опыте компании «Инфосистемы Джет», что подтвердил в своем докладе директор дирекции ИТ «Компании объединенных кредитных карточек» (КОКК — UCS) Сидоров Д.В.

Особое внимание докладчики уделили международным требованиям к защите данных держателей платежных карт, установленным стандартом PCI DSS. В ходе обсуждений посетители

семинара пришли к выводу, что достижение соответствия требованиям PCI DSS — не просто выполнение требований регулирующих органов. Это повышение устойчивости внутренних бизнес-процессов организации. Также специалистами компании «Инфосистемы Джет» были даны разъяснения, касающиеся последствий для финансово-кредитного учреждения в случае несоответствия нормам PCI DSS.

Вторая часть мероприятия была посвящена продуктам и технологиям партнеров компании «Инфосистемы Джет», среди которых были представлены решения компаний Oracle, Symantec и Positive Technologies. Особый интерес у публики вызвал обзор технологий Symantec, направленных на предотвращение утечки персональных данных. Также посетители смогли получить информацию о средствах контроля соответствия внутренним политикам и внешним нормативам по информационной безопасности. Отдельно были представлены функциональные возможности системы управления событиями и инцидентами Symantec Security Information Manager (SSIM).

На организованном в конце семинара «круглом столе» каждый посетитель смог высказать свою точку зрения по вопросам обеспечения непрерывности бизнеса и аварийного восстановления деятельности кредитных организаций после прерываний.

Компания «Инфосистемы Джет» подвела итоги работы Сервисного центра за 2008 год и первый квартал 2009 года

В 2008 году Сервисный центр представил ряд новых услуг и решений: образован Центр Удаленного Мониторинга, расширен спектр обслуживаемых компонентов информационных систем заказчиков, разработано и внедрено уникальное решение — Система раннего предупреждения о сбоях, внедрена новая система ключевых показателей эффективности (KPI).

В дополнение к солидному перечню статусов в 2008 году компания получила статус сервисного партнера от компании EMC — Service-Enabled Value Added Resellers (SE VAR). А в начале 2009 года компания получила два новых партнерских статуса от компании Hitachi Data Systems: Authorised Service Provider (ASP) и Certified Solution Provider (CSP).

В первом квартале 2009 года, несмотря на непростую экономическую ситуацию, Сервисный центр компании «Инфосистемы Джет» продолжил устойчивое развитие.

ТЕМА НОМЕРА

Отчет Symantec об угрозах интернет-безопасности, том XIV

По материалам компании Symantec

Отчет Symantec об угрозах интернет-безопасности

Том XIV «Отчета Symantec об угрозах интернет-безопасности» содержит анализ интернет-деятельности во всем мире, анализ картины интернет-угроз и является единственным общедоступным отчетом подобного рода, который содержит не только глубокий анализ данных и тенденций, но и методологии, используемые для получения этих результатов. Цель отчета состоит в публикации информации, которая помогает потребителям и предприятиям эффективно защищать свои системы сегодня и в будущем.

Этот отчет содержит итоги наблюдения за поведением интернет-угроз в течение 2008 года и основан на крупнейших в мире источниках данных по безопасности:

- Symantec Global Intelligence Network; свыше 240 тыс. датчиков этой сети работает более чем в 200 странах.
- Антивирусные решения Symantec; свыше 130 млн клиентских систем, серверов и шлюзов, на которых установлены антивирусные продукты, присылают отчеты о вредоносных программах, а также о шпионском и рекламном ПО.
- База данных уязвимостей; Symantec ведет одну из самых полных в мире баз данных уязвимостей, которая охватывает свыше 32 тыс. зарегистрированных уязвимостей (более чем за два десятилетия), влияющих на более чем 72 тыс. технологий от более чем 11 тыс. поставщиков.
- BugTraq; один из самых популярных в интернете форумов, который посвящен раскрытию информации и дискуссиям об уязвимостях и имеет около 50 тыс. прямых подписчиков, ежедневно публикующих, читающих и обсуждающих сведения об уязвимостях.
- Symantec Probe Network; система более чем из 2,5 млн учетных записей-приманок, а также Symantec MessageLabs Intelligence и другие технологии Symantec собирают сообщения email более чем в 86 странах и позволяют Symantec измерять деятельность спамеров и фишеров во всем мире; в 16 центрах обработки данных каждый день сканируется 5 млрд сообщений e-mail и более одного миллиарда веб-запросов.
- Symantec Phish Report Network; широкое сообщество по борьбе с мошенничеством, в котором предприятия, поставщики ПО безопасности и более 50 млн потребителей сообщают о мошеннических веб-сайтах, и эти данные используются для сигнализации и фильтрации в широком спектре решений.

Основные обращения

XIV том «Отчета Symantec об угрозах интернет-безопасности» указывает на следующие тенденции:

- Усиление вредоносной деятельности в странах с быстрорастущей инфраструктурой интернета.
- Главным вектором вредоносной деятельности в интернете являются веб-атаки.

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	Germany	14%	18%	6	1	1	2	2
2	2	United Kingdom	11%	11%	1	7	2	6	1
3	4	Spain	9%	8%	4	5	7	1	4
4	5	Italy	8%	8%	5	3	8	3	5
5	3	France	7%	9%	2	8	5	7	3
6	6	Poland	6%	6%	12	6	4	4	8
7	7	Turkey	6%	4%	7	2	13	5	6
8	8	Russia	6%	4%	9	4	3	10	7
9	9	Netherlands	3%	3%	8	20	6	15	10
10	10	Israel	3%	3%	23	9	9	9	11

- Злоумышленники сосредоточены на взломе систем конечных пользователей с целью финансового обогащения.
- Теневая экономика продолжает процветать и крепнуть.

Для «Отчета об угрозах интернет-безопасности» используются данные, собранные из самых обширных источников информации о деятельности в интернете, которые представляют собой уникальное по своему размеру, охвату и четкости полное собрание сведений.

Том XIV «Отчета Symantec об угрозах интернет-безопасности» состоит из шести частей:

- Глобальный отчет об угрозах интернет-безопасности;
- Отчет об угрозах интернет-безопасности по региону EMEA (Европа, Ближний Восток и Африка);
- Отчет об угрозах интернет-безопасности по региону APJ (Азиатско-Тихоокеанский регион);
- Отчет об угрозах интернет-безопасности в секторе государственного управления, который сосредоточен на угрозах, представляющих особый интерес для секторов государственного управления и критической инфраструктуры;
- Отчет об угрозах интернет-безопасности в секторе финансовых услуг;
- Отчет об угрозах интернет-безопасности в регионе Латинской Америки.

В совокупности эти компоненты освещают региональные различия в картине интернет-угроз, а также иллюстрируют, как вредоносная деятельность в разных регионах отражается на глобальных тенденциях и отражает эти тенденции.

Основные обращения с фактами

Вредоносная деятельность усиливается в странах с быстрорастущей инфраструктурой интернета

В 2008 году сократилась доля, вносимая в общую картину вредоносной деятельности странами с развитой инфраструктурой широкополосного доступа, и увеличилась доля практически всех остальных стран из первой десятки.

- Вредоносная деятельность обычно направлена на компьютеры, подключенные к интернету высокоскоростными каналами связи, так как такие соединения являются привлекательными мишенями для злоумышленников.
- Широкополосные соединения обеспечивают более высокую скорость передачи данных по сравнению с соединениями других типов, могут работать постоянно и обычно обеспечивают более стабильную связь.
- Три страны, где ведется наиболее активная вредоносная деятельность, — США, Китай и Германия — имеют также развитые и растущие инфраструктуры услуг широкополосного доступа.
- В странах с быстрорастущими интернет-инфраструктурами и растущим числом поль-

2008 EMEA Rank	2008 Global Rank	Country	2008 EMEA Percentage	2008 Global Percentage
1	3	Ukraine	31%	12%
2	4	Netherlands	19%	8%
3	5	Russia	13%	5%
4	6	United Kingdom	11%	5%
5	9	Latvia	4%	1%
6	10	France	3%	1%
7	11	Estonia	3%	1%
8	12	Germany	3%	1%
9	13	Austria	2%	1%
10	14	Sweden	2%	1%

зователей услуг широкополосного доступа интенсивность вредоносной деятельности, вероятно, будет усиливаться до тех пор, пока ей не станут противостоять улучшенные протоколы и усиленные меры безопасности.

Детали и статистика

- Как и в 2007, в 2008 году странами с наиболее активной вредоносной деятельностью стали США, Китай и Германия, вклад которых составил соответственно 23%, 9% и 6%. Однако вклад этих стран уменьшился по сравнению с уровнями 2007 года, составившими 26% для США, 11% для Китая и 7% для Германии.
  - В 2008 году Китай впервые обогнал США по числу абонентов услуг широкополосного доступа, которое составило 83,3 млн или 21% от общемирового числа; США заняли второе место с 20%, а Германия — третье место с 6%.
- За исключением Франции и Италии, все остальные страны из первой десятки продемонстрировали рост уровня вредоносной деятельности по сравнению с 2007 годом. В их числе Великобритания (рост с 4% в 2007 до 5% в 2008 году); Бразилия и Испания (у каждой рост с 3% в 2007 до 4% в 2008 году); а также Турция и Польша (у каждой рост с 2% в 2007 до 3% в 2008 году).

Главным вектором вредоносной деятельности в интернете являются веб-атаки

Распространенность веб-приложений наряду с множеством простых для эксплуатации уязвимостей в веб-приложениях привела к преобладанию угроз на основе веб-технологий.

- Веб-атаки представляют главную угрозу как для компьютерных сетей предприятий, так и для потребителей; скрытая природа таких атак затрудняет борьбу с ними, так как большинство пользователей не подозревает, что они атакованы. В результате организации вынуждены решать трудную задачу обнаружения вредоносного трафика и его фильтрации.
- Так как многие организации опираются на веб-инструменты и приложения для ведения бизнеса, вероятно, что веб будет оставаться главным проводником вредоносной деятельности и кормить разработчиков вредоносных программ.
- Злоумышленники, использующие веб-атаки на уязвимые клиентские системы, больше не должны активно взламывать сети, чтобы получить доступ к этим компьютерам; вместо этого они могут атаковать и взломать веб-сайт и организовать дополнительные атаки на посетителей этого веб-сайта.
- Большинство подобных атак нацелено на определенные уязвимости или пробелы в защите веб-браузеров или других клиентских приложений, которые обрабатывают информацию, поступающую через веб.
- Веб-атаки могут использовать методы социального инжиниринга для склонения жертвы к просмотру вредоносного веб-сайта, но большинство атак эксплуатирует пользующиеся доверием веб-сайты с высоким уровнем трафика.
- Веб-угрозы не только получили широкое распространение, но и стали более изощренными и опасными.

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	P2008 Top Targeted Sector	Percentage of Lures in Country Targeting Top Sector
1	8	Poland	18%	4%	Financial	90%
2	4	France	11%	10%	Financial	74%
3	5	Russia	10%	8%	Financial	54%
4	1	Germany	9%	15%	Financial	70%
5	2	United Kingdom	9%	%13	Financial	77%
6	6	Italy	6%	8%	Financial	57%
7	3	Netherlands	6%	11%	Financial	57%
8	7	Israel	5%	6%	Financial	63%
9	9	Spain	5%	3%	Financial	71%
10	11	Turkey	3%	2%	Financial	81%

- Динамические сайты служат главными мишенями для злоумышленников, которые используют бот-инфицированные компьютеры для распространения и хранения вредоносного контента, так как эти сайты могут подвергаться риску из-за уязвимости определенных приложений и сайтов.

Детали и статистика

- В 2008 году 63% выявленных уязвимостей влияли на веб-приложения, это больше, чем 59% уязвимостей, выявленных в 2007 году.
- В 2008 году было зарегистрировано 12 885 уязвимостей типа межсайтового скриптинга против 17 697 в 2007 году.
  - Однако среди уязвимостей, о которых было сообщено в 2008 году, всего 394 — или 3% от всех уязвимостей типа межсайтового скриптинга — были исправлены к моменту составления отчета.
  - В 2007 году 1270 уязвимостей типа межсайтового скриптинга — или 7% от всех таких уязвимостей — были исправлены к моменту составления отчета.
- В 2008 году привлекательной мишенью для злоумышленников оставались веб-браузеры, причем в них было зарегистрировано 232 новые уязвимости — меньше, чем в 2007 году (245 новых уязвимостей); однако по сравнению с 2007 годом в 2008 году средняя степень опасности была присвоена большей доле от общего числа уязвимостей веб-браузеров.
  - Из всех уязвимостей браузеров 2008 года 141 была присвоена средняя степень опасности и 91 — низкая; в 2007 году 89 уязвимостей браузеров были признаны уязвимостями средней опасности и 154 — низкой.
  - Эта тенденция к увеличению числа уязвимостей средней степени опасности в браузерах может указывать на повышение квалификации специалистов по безопасности и злоумышленников.
- В 2008 году главным источником веб-атак против пользователей были компьютеры из США — их доля составила 38% от общего числа; второе место занял Китай с 13% и третье место — Украина с 12%.
  - Стоит отметить также, что шесть из десяти стран — главных источников веб-атак находятся в регионе EMEA, на долю которого приходится 45% всех атак — больше, чем на долю любого другого региона.
  - Одной из причин повышенной доли региона EMEA могут быть пакеты эксплойтов; многие такие пакеты (включая MPack, IcePack и NeoSploit) созданы в России, и вероятно, что именно русские, разработавшие эти наборы для организации атак, в большой мере несут также ответственность за их продолжающееся распространение.

Злоумышленники больше, чем когда-либо прежде, сосредоточены на взломе систем конечных пользователей с целью финансового обогащения

Злоумышленники охотятся не за компьютерами конечных пользователей, а за информацией.

- В 2008 году больше угроз, чем в 2007, экспортировали данные или содержали средства перехвата нажатий клавиш.

2008 EMEA Rank	2007 EMEA Rank	2008 Global Rank	Country	2008 EM EA Percentage	2007 EMEA Percentage
1	3	2	Russia	13%	10%
2	8	3	Turkey	12%	4%
3	1	6	United Kingdom	715%	15%
4	4	7	Germany	6%	9%
5	5	8	Italy	6%	6%
6	2	9	Poland	6%	10%
7	111	10	Burundi	5%	<1%
8	6	11	Spain	5%	6%
9	7	14	France	4%	6%
10	20	20	Romania	3%	1%

- Фишеры использовали для заманивания пользователей на свои сайты главным образом фальшивые бренды поставщиков финансовых услуг.
- Некоторые вредоносные программы специально предназначены для раскрытия конфиденциальной информации, которая хранится в зараженном компьютере.
- Эти угрозы могут раскрывать такие важные данные, как сведения о системе, конфиденциальные файлы и документы или верительные данные, тогда как другие могут предоставлять удаленному злоумышленнику полный доступ к взломанному компьютеру.
- Раскрытие конфиденциальной информации на предприятии может привести к серьезной утечке данных; если среди них будут данные о клиентах, такие, как номера кредитных карт, это может серьезно подорвать доверие клиентов к этому предприятию; такое предприятие может нарушить также местные законы.

Детали и статистика

- В 2008 году 78% угроз для конфиденциальной информации экспортировали данные пользователей, против 74% в 2007 году; такие угрозы приносят злоумышленникам пользу, так как собранные данные можно применять для кражи персональной информации пользователей или для организации новых атак.
- В 2008 году угрозы для конфиденциальной информации с возможностью регистрации нажимаемых клавиш — которую можно использовать для кражи такой информации, как реквизиты онлайновых банковских счетов — составили 76% всех угроз для конфиденциальной информации, против 72% в 2007 году.
- В 2008 году 76% фишинговых атак были нацелены на бренды в секторе финансовых услуг; этот сектор продемонстрировал также самый большой уровень кражи персональных данных в результате утечек данных, 29% от общего числа.
  - Аналогично, 12% всех случаев утечки данных, произошедших в 2008 году, были связаны с раскрытием информации о кредитных картах.
  - Не удивительно, что большая часть фишинговой деятельности нацелена на бренды из финансового сектора, учитывая, что 44% пользователей интернета в США, 64% в Канаде и 46% во Франции выполняют те или иные банковские операции, которые могут потребовать ввода номера кредитной карты или реквизитов банковского счета.

Теневая экономика продолжает процветать и крепнуть, несмотря на мировой экономический кризис

Используя данные «Отчета о теневой экономике», Symantec обнаружила, что теневая экономика хорошо организована, имеет профессиональные кадры и процветает.

- Теневая экономика настолько хорошо организована, что такие товары, как чистые пластиковые карты с магнитной полосой, могут изготавливаться в одной стране, пересылаться в другую для записи краденых реквизитов кредитных карт, а затем переправляться в страны, откуда исходят эти краденые данные.

- Профессионализация теневой экономики очевидна из примера Russian Business Network, которая, как известно, специализируется на распространении вредоносного кода, услугах хостинга вредоносных веб-сайтов и т.п.; RBN действовала настолько успешно, что ей приписывают почти половину всех инцидентов фишинга, случившихся во всем мире в 2008 году.
- На укрепление теневой экономики указывает создание псевдокорпораций, где разработка вредоносного кода поставлена на широкую ногу с привлечением большого числа программистов, как при разработке приложений на легитимных предприятиях.
- В отличие от мировой экономики, где в 2008 году наблюдалось падение цен, цены на товары и услуги теневой экономики остаются неизменными.
- Распространение товаров и услуг, рекламируемых на серверах теневой экономики, попрежнему сконцентрировано на финансовой информации, что предполагает, что преступники сильнее сосредоточены на приобретении товаров, которые позволяют им быстро делать большие деньги, чем на эксплойтах, которые требуют больше времени и ресурсов.

Детали и статистика

- Данные кредитных карт возглавляют список товаров и услуг, рекламируемых преступниками в теневой экономике, — на их долю приходится 32% от всех товаров и услуг, против 21% в 2007 году.
- Информация о банковских счетах — вторая по популярности категория товаров, рекламируемых в теневой экономике; на ее долю приходится 19% всех рекламируемых товаров и услуг, против 17% в 2007 году.
- Symantec зафиксировала 55 389 хост-серверов фишинговых веб-сайтов, против 66% в 2007 году, когда было зарегистрировано 33 428 таких хост-серверов; этот рост, вероятно, связан с продолжающимся использованием автоматических фишинговых инструментов, которые ускоряют и автоматизируют процесс создания фишинговых сайтов.
- Цена краденой информации о кредитных картах в 2008 оставалась неизменный на уровне от $0,06 до $30 за карту.
- Цена краденых реквизитов банковского счета в 2008 оставалась неизменный на уровне от $10 до $1000 за счет.

«Комбайн», стоящий на «Конечной Точке»

Алексей Воронцов,
отдел поддержки продаж ЦИБ компании «Инфосистемы Джет»

«Конечные точки» — так называют главную головную боль любого безопасника и айтишника — компьютеры сотрудников организации. Конечные пользователи — самая широкая, самая плохо контролируемая территория, с одной стороны. В массе своей они не подкованы с точки зрения безопасности, да и, зачастую, с точки зрения элементарной компьютерной грамотности, неаккуратны при обращении с информацией, ставят на свои рабочие станции программное обеспечение для развлечения в рабочее время, да и мало ли что еще.

А с другой стороны — это основной состав организации, выполняющий свою работу, в том числе — зарабатывающий компании деньги. Вся построенная ИТ-инфраструктура, по сути, является лишь инструментом для них, конечных пользователей. И все усилия компании, предназначенные для защиты информации, ей принадлежащей, в конечном итоге усложняют работу этих самых конечных пользователей, уменьшая комфорт работы, заставляя совершать лишние операции и, в конечном итоге, снижая производительность их труда. Это напрямую ведет к финансовым потерям.

Уже не первый год компании, специализирующиеся в области информационной безопасности, ведут работу по консолидации различных продуктов для защиты «конечных точек» в единое решение. Продукты по удаленному доступу обрастают антивирусами и шифрованием (как, к примеру, CheckPoint Endpoint Security), продукты класса персональных систем обнаружения/предотвращения вторжения получают функциональность антивируса и контроля конечных устройств (пример: Cisco Security Agent 6). Не стала исключением и компания Symantec, выпустив в 2008 году на смену устаревающему продукту Symantec Antivirus версии 10 продукт с названием Symantec Endpoint Protection 11. Новое в нем оказалось не только название.

Данный продукт ведет свой род от антивирусов, и классический сигнатурный антивирус, предназначенный для корпоративного использования, остается важной его частью. Но эта часть не является единственной (мало того, она не является обязательной — функциональные компоненты нового продукта могут быть установлены по частям). Остальной функционал ведет свои родословные от таких продуктов, как: Symantec Client Security 3, Symantec Sygate Enterprise Protection 5, Symantec WholeSecurity и соответствующих средств управления — Symantec Policy Manager и Symantec System Center. Объединив функции данных продуктов под одной крышей, Symantec Endpoint Protection получил функции персонального межсетевого экрана и системы обнаружения/предотвращения вторжения, контроля внешними устройствами, управления доступом к сети.

Итак, давайте рассмотрим подробнее, что нам это дает.

Персональный межсетевой экран на базе правил работает на сетевом и транспортном уровне. Интересная особенность — возможность указывать в правилах в качестве условия текущее местонахождение компьютера (определяется по одному или нескольким признакам, благодаря чему можно задавать различные правила для нахождения компьютера в корпоративной сети при домашнем подключении, удаленном подключении через VPN и т.д.).

Персональная система обнаружения/предотвращения вторжения. Поведенческие сигнатуры системы очень похожи на сигнатуры Snort. Данный функционал позволяет анализировать поведения приложений, управлять исполнением файлов и загрузкой библиотек. Также существует возможность блокировать мета-классы эксплойтов (в терминалогии Symantec — Generic Exploit Blocking). В сочетании с антивирусом и

персональным межсетевым экраном дает достаточно неплохую защиту от так называемых 0-day атак (эксплуатация неизвестных уязвимостей, для которых нет готовых сигнатур и патчей).

Управление периферийными устройствами. Данная функциональность уступает по возможностям отдельным решениям, но минимальный набор функций предоставляет. Блокирование периферийных устройств, возможность выборочного блокирования чтения, записи, исполнения для внешних устройств — базовый минимум для подобных решений.

Управление доступом к сети. Symantec Endpoint Protection содержит клиент для реализации концепции NAC в видении Symantec. При этом клиент является вполне самодостаточным (к примеру, проверка на наличие антивируса/антиспама/персонального МСЭ проводится для большинства продуктов ведущих поставщиков подобных решений, а не только для составных частей SEP-а).

Все описанные выше функции безопасности управляются из единой консоли и устанавливаются в едином центре. Консоль управления была переписана на основе Java, общение системы управления и компонент идет посредством протокола https. Утрата консоли mmc (Microsoft Management Console, стандартная консоль управления Windows), однако, не повлияла на возможность интеграции с Microsoft Active Directory. Среди возможностей, которые стоит отметить, сетевой сканер, позволяющий находить компьютеры с установленным/неустановленным антивирусом и проводить апгрейд или установку в несколько кликов мыши.

А что для тех самых конечных пользователей? Много функций и, при этом, единый пользовательский интерфейс управления всеми компонентами (см.рис.1). Вдобавок уменьшенное потребление ресурсов (весь комплект Symantec Endpoint Proitection потребляет памяти меньше, чем ранее один Symantec Antivirus, при прочих равных). Повышение производительности коснулось и антивируса, в том числе в режиме сканирования. Впрочем, повышение производительности — это общий тренд для традиционных антивирусов.

И, наверное, главный аспект — весь «комбайн» предлагается как замена 10-й версии антивируса просто по программе апгрейда (см.рис.2). Все текущие пользователи 10-й версии получили уведомления о возможности перехода на новую версию, и многие компании уже провели процедуру апгрейда или рассматривают подобную возможность.

Продукт позволяет апгрейдиться «по частям», сохраняя параллельно серверам управления

Рис. 1. Единый интерфейс пользователя для всех функций защиты

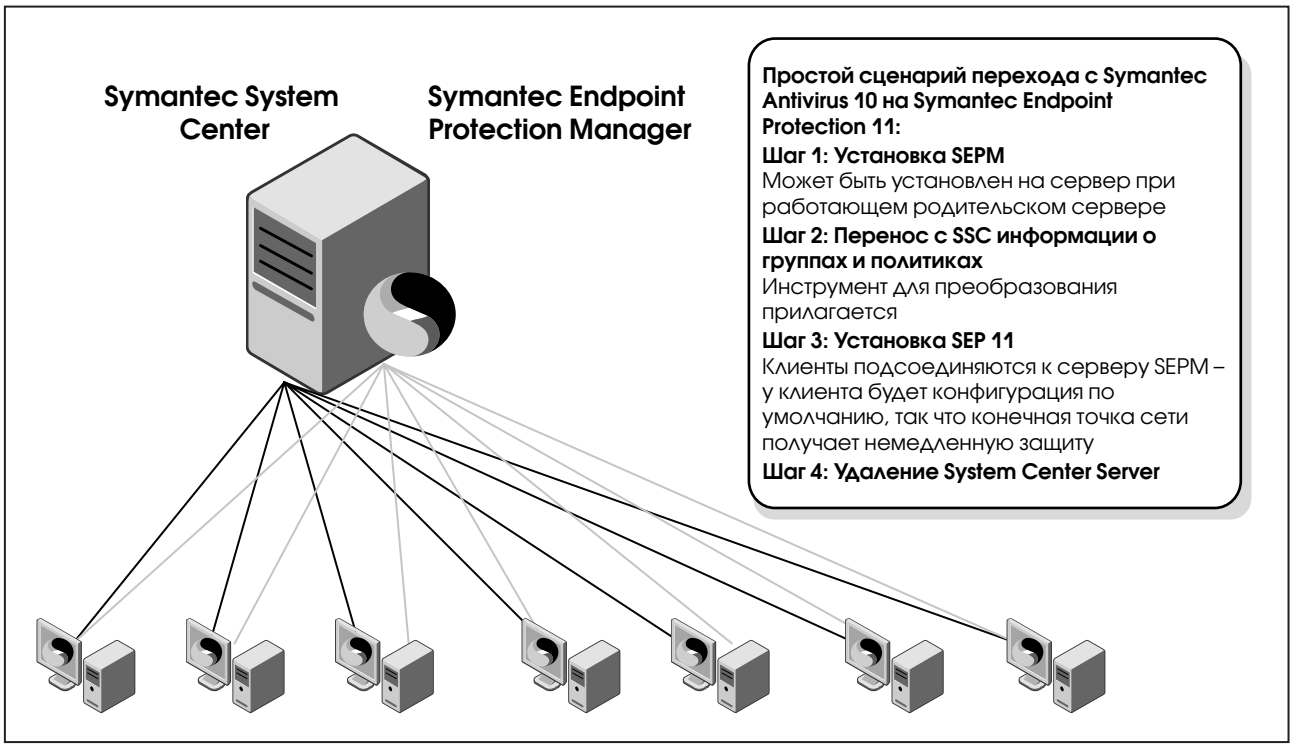


Рис. 2. Перейти с антивируса на комплексную защиту не так сложно

11-й версии старые сервера от 10-ки и постепенно переводя пользователей с одной версии на другую. Большинство крупных заказчиков на моей памяти, особенно имеющих сложные разветвленные локальные сети с множеством филиалов и количеством пользователей в несколько десятков тысяч и выше, поступают именно так. Благодаря этому можно минимизировать поток обращений в службу технической поддержки, который при подобных масштабах апгрейда может быть велик даже для самого совершенного продукта. Кроме того, не обходится и без некоторых особенностей. К примеру, в новой версии была исключена поддержка платформы Itanium и поддержка компьютеров под управлением Novell Netware, присутствовавшие в 10-й версии. Тем компаниям, у которых присутствуют сервера или рабочие станции на подобных платформах, рекомендуется оставить на них 10-ю версию, сохранив параллельно обе инфрастуктуры: старую и новую.

Итак, что мы имеем в сухом остатке? Более функциональный продукт пришел на смену старому и предлагает не только новые функции безопасности, но и дополнительный комфорт простым пользователям. Мало того, весь комплект стоит столько же, сколько стоил раньше один антивирус, и предоставляется по программе подписки взамен старого антивируса Symantec. Что это, бесплатный сыр в мышеловке? Вовсе нет, всего лишь следствие законов рынка. Все лидирующие компании выдвинули свои «комбайны» на передовую «конечных точек». Компания «Symantec» не осталась в стороне, предложив свой вариант. Как всегда от подобного конкурентного взаимодействия мы, конечные пользователи, только выигрываем. Что показывает в том числе и возросшее количество крупных компаний из различных областей деятельности, выбравших за прошедший год именно «комбайн» вместо набора отдельных продуктов. Сокращение издержек за счет поддержки единого решения вместо комплекта разрозненных, уменьшение обращений в техподдержку и жалоб пользователей, увеличение функциональности — основные причины подобных переходов.

Центр оперативного управления ИБ – гарантия и уверенность в уровне обеспечения информационной безопасности

Мария Датриева,
руководитель направления по созданию Центров мониторинга ИБ,
ЦИБ компании «Инфосистемы Джет»

На сегодняшний день главной целью злоумышленников является не просто взлом сети или проникновение в систему, а извлечение прибыли. И хотя для защиты своих информационных активов компании используют различные меры по обеспечению ИБ, тем не менее, инциденты, связанные с информационной безопасностью, и в первую очередь с кражей данных, все равно происходят.

Дело в том, что внедрение только средств защиты, как правило, не гарантирует высокую степень защищенности. В результате нет понимания, насколько полученный уровень информационной безопасности соответствует требуемому, а значит и насколько эффективна вся система обеспечения ИБ в целом. Внутренние и внешние аудиты не являются достаточными для решения данной задачи, поскольку носят периодический характер. Компании, внедряя основные элементы безопасности, зачастую не уделяют должного внимания такому важному элементу обеспечения ИБ, как мониторинг системы информационной безопасности. В результате, затратив силы и средства на внедрение средств защиты, компании считают задачу выполненной, но на проверку оказывается, что:

- критичные системы уязвимы и доступны для злоумышленников;
- на рабочих станциях установлено неразрешенное ПО;
- конфигурации не соответствуют разработанным частным политикам;
- события, свидетельствующие об инциденте ИБ, остаются незамеченными;
- выявив инцидент ИБ, нет четко определенной процедуры, что с ним делать дальше и кто этим должен заниматься;
- у администраторов информационной безопасности нет полной и целостной картины о состоянии ИБ, есть только фрагментарные представления;
- и т.д.

Большинство таких фактов можно было бы избежать, если бы в компании был реализован комплексный мониторинг ИБ, своевременное выявление инцидентов, реагирование на них и эффективное разрешение.

Комплексный мониторинг ИБ подразумевает сбор и анализ событий безопасности от различных систем защиты, устройств и приложений, сбор конфигурационных данных, данных об уязвимостях и т.д. Это позволяет получить полную и достоверную информацию об имеющихся событиях и уязвимостях ИБ, текущих настройках, т.е. иметь целостную картину текущей защищенности компании. Осуществляя такой контроль, организации имеют возможность оперативного управления информационной безопасностью, исправляя выявляемые отклонения, своевременно разрешая инциденты ИБ, устраняя уязвимости, принимая меры по корректировке средств защиты и т.д.

Подтверждение важности и необходимости комплексного мониторинга нашло отражение в различных стандартах в области информационной безопасности, таких, как: PCI DSS, ISO/IEC 27001:2005, SOX, Basel II, СТО БР ИББС-1.0-2006, СТР-К.

Централизация оперативного управления ИБ

Собранная в ходе комплексного мониторинга информация поступает в единый центр, где она обрабатывается и представляется в наглядном и удобном виде. Здесь же осуществляется реагирование и разрешение инцидентов ИБ, устранение выявленных отклонений. Построение такого **Центра оперативного управления ИБ (Security Operations Center, SOC (см.рис.1))** является непростой задачей.

Центр оперативного управления ИБ позволяет контролировать и оперативно управлять информационной безопасностью компании в режиме реального времени, быть уверенным в том, что требуемый уровень обеспечения ИБ достигнут и поддерживается, отслеживать выполнение заданных целевых показателей эффективности (KPI) обеспечения ИБ.

Центр оперативного управления ИБ позволяет отслеживать происходящие в информационной системе события, связанные с ИБ, анализировать и сопоставлять их с другими данными, представлять собранную информацию в наглядном и удобном виде, контролировать имеющиеся уязвимости, осуществлять контроль конфигураций, отслеживать степень выполнения требований законодательства, нормативных актов и корпоративных политик, а также оперативно реагировать на выявленные инциденты ИБ. То есть предоставляет полную картину текущего состояния информационной безопасности компании, что позволяет оперативно устранять выявляемые отклонения и обеспечивать заданный уровень ИБ.

Ключевыми факторами, обеспечивающими эффективность подобных центров, являются: внедрение процессов мониторинга, управления уязвимостями и инцидентами, правильное разграничение ответственности между сотрудниками внутри компании, разработка и внедрение регламентов реагирования на инциденты ИБ и их последующего разбора.

В многофилиальных компаниях с развитой ИТ-инфраструктурой и большим количеством разнообразных средств защиты без специализированных технических средств реализовать полноценный комплексный мониторинг ИБ весьма проблематично.

Также многое зависит от качества настроек технических средств и квалифицированных действий обслуживающего персонала.

Внедряя Центр оперативного управления ИБ, компании одновременно реализуют часть процес-

Рис. 1. Центр оперативного управления ИБ

сов системы управления ИБ (СУИБ) в соответствии со стандартом ISO27001 (процесс управления инцидентами ИБ, управление уязвимостями, управление изменениями, контроль соответствия законодательным и отраслевым требованиям), а также выполняют часть требований стандарта PSI DSS (требования разделов 1, 6, 10, 11, 12).

Таким образом, **Центр оперативного управления ИБ** представляет собой набор связанных и работающих процессов управления ИБ (мониторинг, управление инцидентами, управление уязвимостями, инвентаризация активов, управление изменениями, контроль политик безопасности) и автоматизирующих их технических систем:

- Мониторинга состояния ИБ:
  - мониторинг событий ИБ;
  - аудит действий пользователей;
  - управление уязвимостями/контроль конфигураций;
- Управления инцидентами ИБ;
- Контроля соответствия требованиям законодательства, международных и отраслевых стандартов, внутренних корпоративных политик.

Мониторинг состояния ИБ

Система управления (мониторинга) событиями ИБ (Security Information Management System, SIMS) — реализует комплексный подход к решению задач сбора, анализа (корреляции) и контроля событий ИБ от различных средств защиты, что позволяет в режиме реального времени эффективно идентифицировать инциденты информационной безопасности (с дальнейшей их передачей в систему управления инцидентами), получать реальные данные для анализа и оценки рисков, для принятия обоснованных и адекватных имеющимся рискам решений по обеспечению ИБ.

Система управления событиями ИБ помогает решить следующие задачи:

- управление большим объемом событий ИБ;
- получение полной картины происходящего в ИС;
- мониторинг текущего уровня обеспечения безопасности (контроль достижения заданных показателей эффективности (KPI) обеспечения ИБ);
- своевременное обнаружение инцидентов ИБ;
- получение реальных данных для анализа и оценки рисков;
- принятие обоснованных решений по управлению ИБ;
- выполнение требований законодательства и нормативных актов по мониторингу событий, связанных с ИБ (ISO/IEC 27001:2005, SOX, Basel II, PCI DSS, СТО БР ИББС-1.0-2006, Федеральный закон о персональных данных (№512-ФЗ), СТР-К, ГОСТ Р ИСО/МЭК 17799-2005).

На рынке систем управления событиями информационной безопасности представлены технические решения различных производителей, они отличаются по функционалу, спектру решаемых задач, сфере применения:

- Symantec Security Information Manager (SSIM);
- nFX SIM One (netForensics);
- ArcSight Enterprise Security Management (ArcSight ESM);
- Cisco Security Monitoring, Analysis and Response System (CS-MARS).

Система аудита действий пользователей обеспечивает регистрацию и анализ действий пользователей (прежде всего на уровне БД), рассылку уведомлений в режиме реального времени и подготовку отчетов о том, кто получает доступ, к какой именно информации, и как эти действия могут нарушить требования внешних регулирующих органов или внутренние правила по информационной безопасности компании.

Система аудита действий пользователей помогает решить следующие задачи:

- контроль злонамеренных действий пользователей;
- защита от утечки конфиденциальной информации;
- получение ответа на вопросы: «Кто? Что сделал? Когда? Где? Откуда? Куда? С помощью каких средств?»;
- подготовка отчетов различного уровня (от руководителя компании до администратора информационной безопасности).

Для контроля действий пользователей могут быть использованы решения компании Imperva, а также отлично зарекомендовавшие себя продукты nFX Data One (netForensics) и Oracle Audit Vault, первый из которых легко интегрируется с другими продуктами компании netForensics, а второй — разработан специально для одной из наиболее распространенных СУБД — Oracle.

Система управления уязвимостями/контроля конфигураций позволяет получать данные

по имеющимся уязвимостям в режиме реального времени, отслеживать динамику их устранения, контролировать производимые изменения, а также обеспечивает автоматизацию таких задач, как: инвентаризация ресурсов и контроль конфигураций. Поиск уязвимостей критичных ресурсов проводится на постоянной основе различными способами:

- сетевое сканирование;
- тест на проникновение;
- системные проверки;
- анализ защищенности СУБД;
- анализ защищенности Web-приложений.

Система реализуется на базе продукта MaxPatrol (Positive Technologies).

Управление инцидентами ИБ

Система управления инцидентами ИБ осуществляет регистрацию, оперативное реагирование и эффективное разрешение инцидентов ИБ, а также реализует полный цикл работы с инцидентами.

От того насколько быстро и грамотно компания среагирует и разрешит возникший инцидент информационной безопасности, зависит размер ущерба, наносимого ей в результате инцидента, поэтому подготовка к разрешению инцидентов приобретает особое значение.

Подготовительный этап включает планирование, определение ответственных, разграничение обязанностей, разработку планов по разрешению инцидентов и т. д. Далее осуществляется непосредственно регистрация инцидентов ИБ и реагирование на них с последующим разрешением.

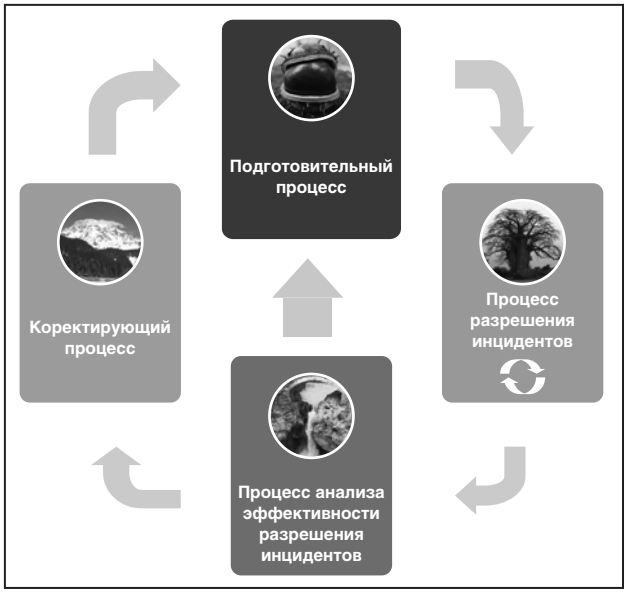


Рис. 2. Управление инцидентами ИБ

В процессе управления инцидентами информационной безопасности важно не только разрешить эти инциденты, но и проанализировать, насколько эффективно осуществляется их разрешение. Необходимо периодически тестировать разработанные планы для поддержания их в актуальном рабочем состоянии и для своевременного улучшения. Кроме того, необходимо проводить анализ произошедших инцидентов с целью дальнейшей корректировки текущих мер защиты и принятия мер проактивной защиты.

Если при анализе выявлены незначительные отклонения, то проводятся корректирующие действия. Если же выявлены системные ошибки, обнаружена неэффективность применяемых планов и т. п., то производится активация подготовительного этапа.

Общая схема управления инцидентами ИБ представлена на рис. 2.

Построение **Системы управления инцидентами ИБ** предполагает внедрение процесса управления инцидентами ИБ и (опционально) его автоматизацию.

Контроль соответствий

Система контроля соответствий позволяет выполнять регулярные технологические проверки соответствия информационных систем внутренним политикам безопасности компании, техническим стандартам, требованиям нормативных актов, международным стандартам и т. п. Результат проверки предоставляется в виде детального отчета.

Данная система предоставляет возможность определить внутренний стандарт на базе:

- международных стандартов (ISO 27001, PSI DSS и др.);
- рекомендаций производителя;
- «Best practice» NSA, NIST, CIS;
- внутренних требований,

а также постоянно контролировать соблюдение стандартов для:

- сетевого оборудования;
- прикладных систем (ERP, CRM);
- операционных систем UNIX и Windows;
- различных СУБД.

Система может быть реализована на базе продуктов MaxPatrol (Positive Technologies) и Control Compliance Suite (Symantec).

Построение Security Operation Center, SOC

Возможны различные варианты построения SOC в зависимости от степени зрелости и текущих задач компании: от внедрения отдельных систем до комплексных решений.

При реализации сложных масштабных проектов в ряде ситуаций оптимально поэтапное внедрение, когда на каждом этапе увеличивается область применения SOC как по территориальному охвату (например, сначала головной офис, затем регионы), так и по функциональным системам (например, сначала система управления событиями ИБ, а затем система управления уязвимостями).

Использование решений нескольких производителей позволяет учесть масштаб, ИТ-инфраструктуру и другие особенности каждой компании. Примеры использования SOC приведены в таб. 1.

Выгоды, получаемые компанией при внедрении SOC

- Непрерывное усовершенствование защитных мер для обеспечения безопасности: постоянный анализ текущих событий и инцидентов ИБ, выяснение причин их возникновения с привлечением различных подразделений, позволяет оценить эффективность текущих мер защиты, понять их недостатки и

Таб. 1. Использование Центра оперативного управления ИБ для решения задач бизнеса

Задачи бизнеса	Решение с помощью SOC
Сокращение расходов и потерь	Создание Центра оперативного управления позволят сократить расходы за счет централизации управления, а также снизить ущерб, наносимый в результате возникновения инцидентов ИБ, за счет своевременного и эффективного реагирования. Использование процессного подхода делает реагирование и разрешение инцидентов информационной безопасности более оперативным и позволяет использовать как собственный, так и мировой опыт по разрешению инцидентов ИБ.
Повышение стоимости компании	Центр оперативного управления ИБ повышает управляемость и стабильность компании, что ведет к увеличению ее стоимости. Это становится особенно актуально, когда речь идет о слиянии и поглощении. Потенциальный собственник предпочитает понимать, какие инструменты используются для оперативного управления ИБ, ценит использование комплексного и системного подхода для решения задач информационной безопасности.
Соответствие требованиям законов и нормативных актов как российских, так и международных	Наличие Центра оперативного управления свидетельствует о выполнении требований и рекомендаций по мониторингу и управлению инцидентами ИБ, прямо или косвенно присутствующих как в международных стандартах и нормативных актах (ISO/IEC 27001:2005, PCI DSS, Basel II, Sarbanes-Oxley Act), так и в российских (СТО БР ИББС-1.0-2006, Федеральный закон о персональных данных (№512-ФЗ), СТР-К, ГОСТ Р ИСО/МЭК 17799-2005).
Управление операционными рисками	Контроль операций и контроль конфигураций являются составляющими управления операционными рисками. Центры оперативного управления ИБ осуществляют мониторинг всех производимых действий, отслеживают факты изменений конфигурационных настроек, контролируют их соответствие установленным в компании требованиям, политикам. Центр оперативного управления может быть использован как средство автоматизации при анализе рисков, предоставляя реальные данные о текущих уязвимостях и угрозах.

выработать предложения по их замене или корректировке.

- Снижение затрат: при небольшом штате сотрудников, когда «не хватает рук», SOC позволяет сократить ресурсы, требуемые при ручной обработке событий ИБ и при увеличении количества контролируемых средств защиты, не требует увеличения штата, а напротив, путем сведения данных на одну консоль и автоматизации проводимого анализа событий ИБ, позволяет оптимизировать работу сотрудников.
- Разделение полномочий контроля за ИТ-системами: средства защиты, их администрирование и эксплуатация, как правило, находятся в ведении подразделения ИТ, в то время как ИБ отводятся только функции контроля. SOC — это, пожалуй, единственный инструмент контроля в руках у подразделений ИБ, позволяющий им отслеживать действия в ИТ-системах, что объективно снижает влияние человеческого фактора и повышает уровень информационной безопасности компании.
- Оптимизация слияния компаний: SOC позволяет эффективно привести присоединяемую компанию в соответствие со стандартами ИБ, принятыми в головной компании. SOC дает возможность не только оперативно обнаружить расхождения, но и отследить их устранение с возможностью выставления и контроля соответствующих KPI ответственным за слияние подразделениям.
- Оптимизация затрат на обеспечение ИБ: данные, предоставляемые SOC, существенно уточняют оценку рисков, которая является основой в выборе тех или иных мер защиты. Кроме этого, формализация процедур снижает косвенные затраты компании, т. к. вопросы согласований без качественного обоснования занимают значительное количество рабочего времени сотрудников.

Построение Центра оперативного управления ИБ на базе продуктов компании Symantec

Для построения Центров оперативного управления ИБ используются решения нескольких производителей, что позволяет учесть масштаб, ИТ-инфраструктуру и другие особенности каждой компании.

Рассмотрим построение Центра оперативного управления ИБ на базе продуктов компании Symantec:

- Symantec Security Information Manager (Symantec SIM);
- Symantec Control Compliance Suite (Symantec CCS).

Symantec SIM используется для комплексного мониторинга и автоматизации процесса управления инцидентами ИБ, а Symantec CCS для контроля политик безопасности. Оба продукта хорошо интегрируются друг с другом и объединены в единое решение в 9-ой версии продукта Symantec Control Compliance Suite.

Эти продукты можно также использовать для закрытия соответствующих требований при выполнении проектов по PCI DSS и СТО БР ИББС-1.0.

Symantec Security Information Manager

Основные задачи, решаемые Symantec SIM:

- управление событиями ИБ;
- управление инцидентами ИБ;
- контроль активности пользователей;
- контроль состояния безопасности компании.

Основные возможности Symantec SIM представлены ниже.

Сбор данных и анализ безопасности в режиме реального времени

Продукт Symantec SIM осуществляет централизованный сбор событий ИБ от программно-технических средств более, чем 100 различных производителей. Для «неподдерживаемых» систем есть возможность разработки собственных коллекторов для сбора событий ИБ при помощи специализированного программного пакета Collector Studio.

На основе собранных данных Symantec SIM помогает выявлять угрозы безопасности, направленные на наиболее важные бизнес-приложения, определять их приоритеты, анализировать и устранять эти угрозы.

Сопоставление недостатков защиты сети и хостов в режиме реального времени с помощью службы Symantec Global Intelligence Network — это одно из ключевых преимуществ продукта Symantec SIM, делающее его системой оперативного реагирования на инциденты мирового класса с акцентом на обеспечение безопасности наиболее важных для бизнеса информационных ресурсов.

Symantec Global Intelligence Network — глобальная сеть, использующая ловушки для обнаружения злонамеренной активности по всему миру. Большое внимание уделяется анализу подозрительной активности по различным портам/протоколам. Исследуются приложения, использующие эти порты/протоколы, проверяется, не были/появлялись ли новые уязвимости в этих приложениях, анализируется вероятность использования приложений в злонамеренных целях. Также создается статистика наиболее атакующих и атакуемых систем. Вся эта информация перерабатывается в правила и используется в Symantec SIM при анализе и корреляции событий.

Анализ безопасности в режиме реального времени осуществляется с использованием внешнего стандарта выявления угроз безопасности — процесс, описанный в открытых стандартах Distributed Management Task Force (DMTF). Данный метод предусматривает классификацию угроз и проблем безопасности с учетом степени воздействия события на среду, способа атаки и целевых ресурсов. Такая классификация, называемая «Эффекты, механизмы и ресурсы» (EMR), лежит в основе модуля анализа данных Symantec SIM. Благодаря гибкости интеллектуальных правил на основе шаблонов, отдельное правило может занять место нескольких более конкретных правил, применяемых в стандартных подходах. В результате значительно упрощается процедура обслуживания и создания правил, которые могут охватывать множество условий.

В системе заведено большое количество предопределенных правил корреляции, есть возможность создавать свои собственные правила. Можно задавать правила отрицательного усло-

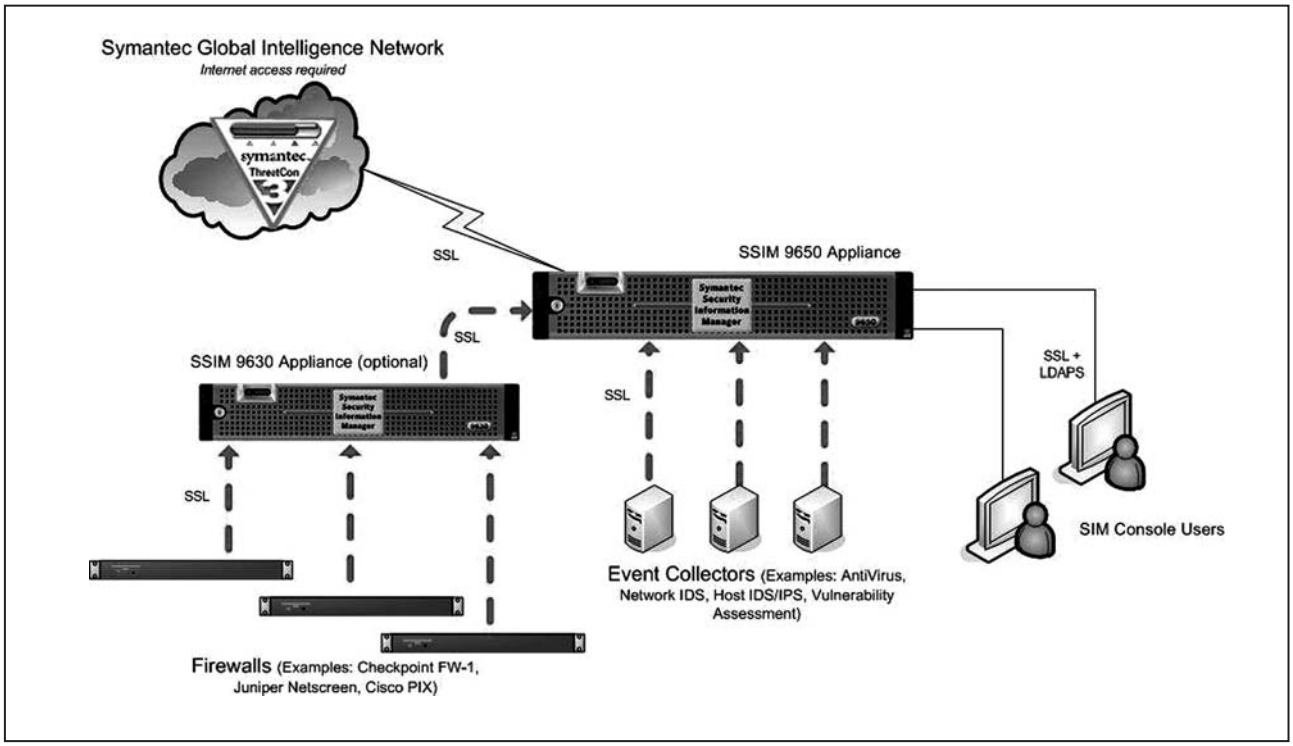


Рис. 3. Архитектура Symantec SIM

вия, которые срабатывают в случае отсутствия события в течение заданного времени. Это очень полезно для контроля поступления событий от определенного источника данных.

Управление инцидентами

На основе созданных правил формируются инциденты ИБ, которые могут быть объединены в иерархию инцидентов. Каждому инциденту назначается приоритет в соответствии с указанными сведениями о защищаемых активах.

В Symantec SIM реализована встроенная система управления инцидентами, позволяющая назначить ответственного за инцидент, эскалировать инциденты, автоматизировать процесс контроля разрешения инцидентов, передать инцидент во внешнюю службу Help Desk для обработки, получить результат его разрешения (обратная связь) и т.д.

Таким образом, продукт Symantec SIM также используется для автоматизации и документирования разрешения инцидентов.

Хранение данных

Кроме сбора данных компании должны соблюдать официальные требования по хранению архивов, обеспечивая надлежащую работу средств хранения и извлечения данных. Продукт превосходит стандартные продукты контроля информации о безопасности на основе реляционных баз данных, для которых характерны дополнительные начальные затраты и необходимость длительного администрирования баз данных. С продуктом Symantec SIM не требуется администрирование базы данных. Продукт сохраняет события в архивных файлах в указанном месте. Архив реализован в виде самостоятельного модуля. Он отслеживает использование диска и срок хранения отдельных архивных файлов. При достижении указанного ограничения дисковой памяти или даты истечения срока действия файла Symantec SIM удаляет старые архивные файлы, чтобы освободить место для новых файлов. Для хранения файлов можно выбрать программно-аппаратный комплекс, напрямую подключенный диск (DAS), сетевое устройство хранения (NAS) или сеть хранения данных (SAN). Архивы Symantec SIM работают быстрее обычных баз данных, поскольку в отличие от нескольких сотен функций базы данных они оптимизированы для выполнения одной задачи — сохранения большого объема событий. Коэффициент сжатия в продукте Symantec SIM достигает 30:1. Нормализованные данные вместе с исходной информацией о событиях фиксируются и сохраняются для анализа происшествий.

Для обеспечения конфиденциальности и целостности архивы имеют электронную подпись.

Отчетность

Продукт Symantec SIM позволяет создавать отчеты для руководителей, технические отчеты и отчеты о контроле, содержащие наглядное представление уровней серьезности угроз и состояния безопасности компании. Предусмотрено более 400 готовых отчетов — от соблюдения требований до различных аспектов защиты. При необходимости с помощью мастера запросов можно создать собственные отчеты. В состав Symantec SIM входят стандартные шаблоны оценки соблюдения требований PCI DSS, SOX и др.

При передаче собранных данных между компонентами Symantec SIM обеспечивается конфиденциальность и целостность передаваемой информации.

Продукт предоставляет возможность его внедрения в различных вариантах, в соответствии с потребностями компании, а также обеспечивает возможность построения резервируемого, распределенного и масштабируемого решения по его внедрению.

Общая архитектура Symantec SIM представлена на рис. 3.

Symantec SIM – PCI DSS

Компания «Инфосистемы Джет» использует продукт Symantec SIM в проектах по PCI DSS для закрытия требований стандарта по отслеживанию всех обращений к сетевым ресурсам и данным о держателях платежных карт (требования раздела 10).

Наличие в продукте возможности разработки собственных коллекторов для сбора событий ИБ, а также поддержка русского языка, позволяет собирать данные с АБС собственной разработки и «неподдерживаемых» на данный момент систем.

Symantec SIM, с одной стороны, является недорогим решением для небольшого отдела процессинга. С другой стороны, в последствие это решение может быть легко масштабировано до размеров всей компании.

Данный продукт уже использовался компанией «Инфосистемы Джет» в ряде банков и входит в состав типового решения в проектах по PCI DSS.

В частности, данное решение было использовано в проекте по приведению процессинговых систем ЗАО «Компания объединенных кредитных карточек» в соответствие с требованиями PCI DSS.

Symantec Control Compliance Suite

Продукт Symantec CCS осуществляет автоматический контроль отклонений от стандартов безопасности и обеспечивает полный охват жизненного цикла задач ИТ-соответствия, включая управление политиками безопасности, оценку технических и административных контролей, отчетность и устранение недостатков.

Подход компании Symantec по управлению соответствием состоит в следующем (рис. 4):

1. Обозначить риски и разработать политики безопасности.
2. Провести оценку инфраструктуры и процессов.
3. Отслеживать и демонстрировать соответствие.
4. Оценить риски и устранить проблемы.

Продукт состоит из 4-х логических элементов: Policy, Response Assessment (RAM), Standards и SIM (описание SIM см. выше).

Встроенный модуль Policy позволяет определить внутреннюю политику вручную или на базе:

- международных стандартов (ISO 27001, PCI DSS и др.);
- рекомендаций производителя;
- «Best practice» NSA, NIST, CIS;
- внутренних требований.

В дальнейшем созданными политиками можно управлять, проверять, утверждать, распространять через web-портал, привязывать к тем или иным стандартам, нормативным документам.

Оценка состояния безопасности и обеспечение соответствия созданным политикам осуществляется для следующих операционных систем и приложений: Windows®, UNIX®, Linux®, NetWare®, SQL Server, Oracle® и Exchange.

Поиск уязвимостей критичных ресурсов и несоответствия конфигурационных настроек проводится на агентной и безагентной основе (рис. 5).

Рис. 4. Управление соответствием CCS

Продукт Symantec CCS позволяет качественно оценить и постоянно контролировать соблюдение стандартов с целью быстрого выявления отклонений (систем, не соответствующих требованиям). Оценка соответствия техническим стандартам посредством подсчета баллов «соответствует/не соответствует», позволяет избежать многочасовых ручных операций по выявлению и анализу отклонений. Ссылка на результаты проверки на соответствие отправляется администратору по электронной почте, так что он может их просмотреть из любой точки ИТ-инфраструктуры с помощью браузера Microsoft Internet Explorer. Благодаря выявлению тенденций на основе логической иерархической группировки и детальному анализу несоответствующих требованиям систем обеспечивается быстрое устранение отклонений. В результате уменьшается риск возникновения несоответствий, брешей в системы безопасности и нарушений в работе бизнеса. По выявленным проблемам создаются всеобъемлющие перечни необходимых мероприятий, например, встроенные рекомендации, списки исправлений, которые необходимо получить из базы данных исправлений Shavlik®. В продукте реализована интеграция с системами обработки запросов, предоставляется возможность задания автоматического исправления выявленных отклонений.

Встроенный модуль Entitlement Manager собирает действующие права доступа к данным по всему предприятию, преобразует их в согласованный и удобочитаемый формат, классифицирует данные и передает информацию о разрешениях для утверждения бизнес-владельцам этих дан-

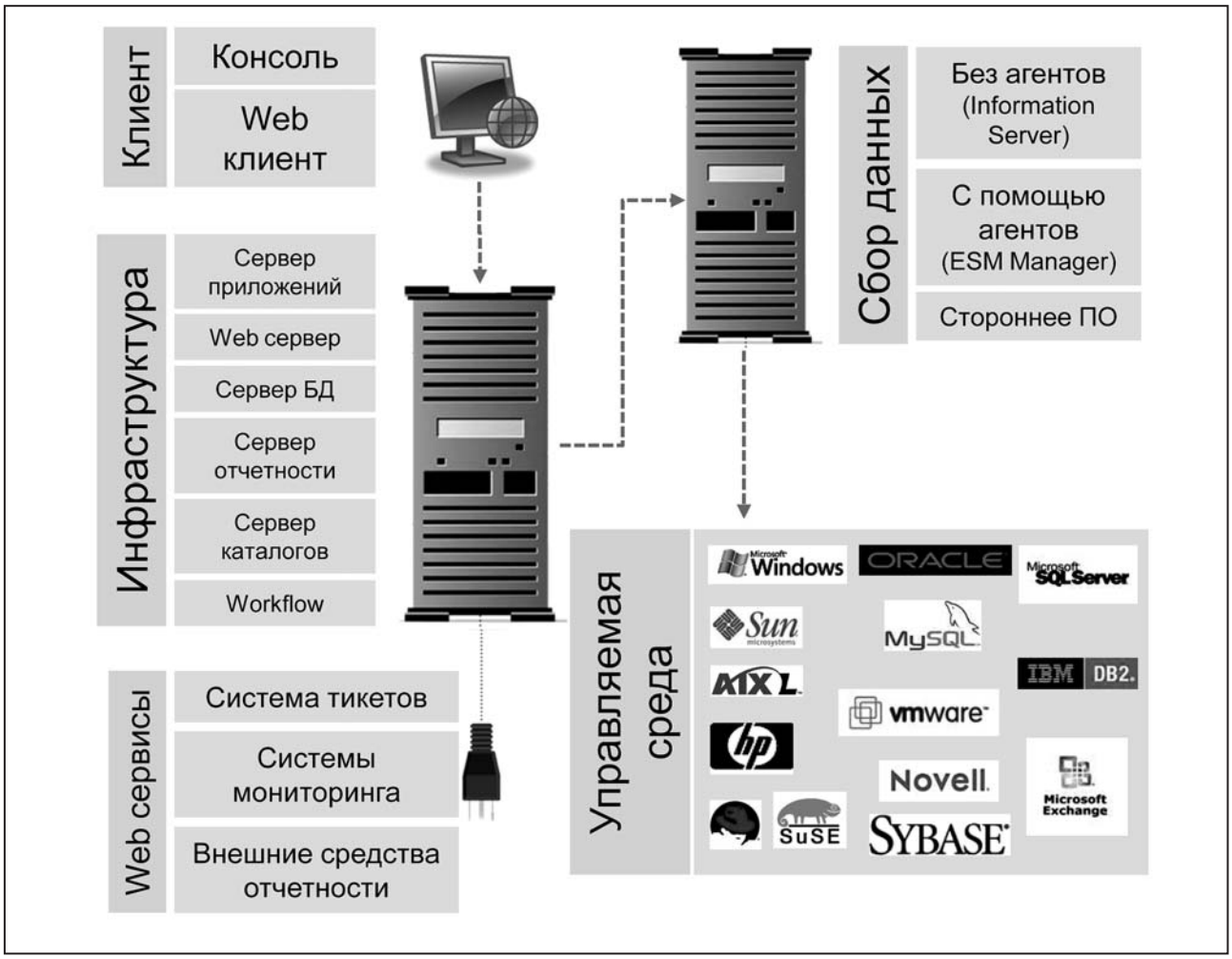


Рис. 5. Общая архитектура CCS 9.0

ных. Предоставляет детальные отчеты о правах, показывающих: «кто имеет доступ к определенной информации», «к какой информации имеет доступ данное лицо» и «кто является бизнес-владельцем этой информации».

Symantec CCS также осуществляет проверку как технических, так и НЕтехнических (административных) контролей. Встроенный модуль Response Assessment (RAM) автоматизирует оценку нетехнических контролей. Большинство объектов, о которых упоминается в нормативных актах и стандартах, представляют собой административные средства управления. Организации часто опираются на оценки на бумаге, составление которых требует больших трудозатрат и которыми трудно управлять. Модуль RAM управляет процессом ручной оценки от создания и распространения анкет до анализа собранных данных:

- Создание из встроенных шаблонов или импорт из документов или создание новых опросов.
- Отслеживание ответов (принятие, запросы на пояснение.
- Создание списков заданий на исправление с указанием владельца задания и конкретных действий.
- и т.д.

При создании опросов есть возможность установить пороговые значения для успешного завершения опроса и количество попыток, а также оценивать результаты и отображать числовые значения в панели анализа. В качестве доказательств прикрепляются документы различных типов (до 3-х документов на вопрос) или даются ссылки. Имена документов и ссылки отображаются в панели анализа, сами документы хранятся в БД SQL, допускается их редактирование / удаление из БД.

В продукте Symantec CCS также реализовано немедленное всеобъемлющее устранение отклонений в виде процедуры с обратной связью, гарантирующей сведение уязвимостей к минимуму: автоматизация управления изменениями в организациях, использующих продукты Remedy® или HP® Service Desk, с возможностью подтверж-

дения полноты и точности корректирующих действий. При проведении оценки соответствия автоматически (или полуавтоматически — требуется просмотр и утверждение пользователем) открываются «инциденты», в продуктах Remedy или HP Service Desk (с помощью встроенного интерфейса). По всем инцидентам, открытым с помощью Symantec CCS, подготавливаются соответствующие отчеты, включая просмотр заметок и состояния.

- Осуществляется контроль итогового статуса «fixed» или «closed» для открытых инцидентов, а также — корректного выполнения требуемых заданий.

Таким образом, продукты CCS и SIM, осуществляя консолидированный обзор текущего соответствия и данных конфигурации (CCS) и мониторинг ИТ-среды в реальном времени (SIM), реализуют комплексный мониторинг ИБ компании. И вместе с внедрением соответствующих процессов управления ИБ (управление инцидентами, управление уязвимостями, инвентаризация активов, управление изменениями, контроль политик безопасности) позволяют построить эффективный Центр оперативного управления информационной безопасностью.

Модернизация локальной вычислительной сети Иркутского авиационного завода

О заказчике

Иркутский авиационный завод (ИАЗ) основан в 1932 году. За семьдесят пять лет на предприятии было освоено производство более двадцати типов самолетов практически всех конструкторских бюро СССР и России. При этом каждый новый тип авиационной техники отличался конструкторскими и технологическими решениями, уникальными для своего времени. Самолеты Иркутского авиационного завода поставлялись в тридцать семь стран мира. В 1997г. завод первым из предприятий авиационной промышленности России получил сертификат соответствия системы обеспечения качества производства международному стандарту ISO 9002.

В настоящее время Иркутский авиационный завод является мощной производственной площадкой ОАО «Научно-производственная корпорация «ИРКУТ», ее главным процессинговым центром, способным выполнять все виды работ по проектированию, производству, реализации и послепродажному обслуживанию авиационной техники военного и гражданского назначения.

27 мая 2008 года корпорация «ИРКУТ» получила сертификат соответствия системы менеджмента качества международным стандартам ISO 9001:2000 & EN/AS 9100:2003.

Задачи

Локальная вычислительная сеть ИАЗ была построена в 2000г. по технологии коммутируемого Ethernet. Волоконно-оптическая инфраструктура объединила шесть объектов завода, расположенных на трех территориально удаленных друг от друга площадках.

За семь лет эксплуатации использовавшееся для построения сети оборудование морально устарело, часто выходило из строя. Сотрудники завода жаловались на перебои в работе сети и недоступность или «медленную работу» бизнес-приложений. Существовавшая конфигурация сети затрудняла подключение новых объектов, площадок.

В начале 2007г. руководство корпорации «ИРКУТ», в рамках программы по обеспечению непрерывности бизнеса, приняло решение о модернизации ЛВС Иркутского авиационного завода.

По результатам проведенного выбора исполнителем проекта стала компания «Инфосистемы Джет». Перед ее специалистами были поставлены следующие задачи:

1. Оптимизировать использование существующих кабельных систем и активного сетевого оборудования.
2. Обеспечить соответствие оборудования новым требованиям к качеству обслуживания для передачи различных типов трафика (голос, данные, видео).
3. Обеспечить требуемую производительность для работы бизнес-приложений.
4. Обеспечить возможность подключения новых объектов сети.
5. Повысить управляемость и отказоустойчивость ЛВС.

Новая ЛВС должна была обеспечить возможность работы устройств и около 4500 пользователей.

Все работы по ее модернизации требовалось проводить без остановки работы существую-

щей сети, поскольку нарушать непрерывность производственных процессов завода было нельзя.

Решение

Специалисты компании «Инфосистемы Джет» провели обследование существующей сети. В результате был разработан техно-рабочий проект построения новой сети с учетом требований по пропускной способности, надежности и масштабируемости, предъявляемых заказчиком. Кроме того, был разработан план выполнения работ по модернизации сети. Специалисты компании «Инфосистемы Джет» предложили выполнять работы поэтапно. Были описаны действия, необходимые для успешного выполнения каждого этапа. Определена критичность этапов и степень влияния проводимых работ на остальную сеть. На основе этих данных были запланированы время проведения работ (ночное, дневное, выходные дни) и необходимые ресурсы. Кроме того, в этом документе были описаны решения по сопряжению новой и существующей сети, а также представлен порядок переключения участков сети, серверных ресурсов, внешних подключений и пользователей.

Модернизированная ЛВС построена по модульному принципу — это обеспечивает масштабируемость системы. Выделены следующие иерархические уровни сети: уровень ядра системы (магистраль сети), уровень распределения и уровень доступа. Архитектура сети разработана с использованием топологии «звезда с двойным центром» — это позволяет исключить наличие единых точек отказа, поскольку оборудование на уровне ядра сети и на уровне подключения серверов резервируется по принципу 1+1. Сеть построена на активном сетевом оборудовании компании Nortel. Ядром сети являются коммутаторы Nortel ERS 8610.

Магистраль сети переведена на технологию 10Gigabit Ethernet с использованием технологий создания логических групп каналов (DMLT, SMLT). Это позволило увеличить пропускную способность ядра сети, повысить надежность решения, обеспечить отсутствие неиспользуемых каналов связи и оборудования.

На Иркутском авиазаводе используются различные типы сетевых приложений:

- бизнес-приложения (SSA ERP LN v.6.1 (BAAN), Teamcenter engineering, СУБД ORACLE, HR-система «БОСС-кадровик» и др.);
- система IP-телефонии;
- система видеоконференцсвязи (ВКС);
- другие сетевые приложения.

Все они имеют различную степень критичности для бизнеса и отличаются требованиями к обеспечению качества обслуживания (QoS). Для обеспечения QoS был применен механизм классификации потоков данных Differentiated Services Code Point (DSCP): каждому типу приложения сопоставлен класс обслуживания, в соответствии с которым коммутаторы ЛВС передают его трафик.

В крупных сетях поиск и устранение неисправностей всегда были непростыми задачами, существенно облегчить решение которых помогают средства оперативного мониторинга и управления. Специалисты компании «Инфосистемы Джет» создали интегрированную систему управления активным сетевым оборудованием на базе продуктов компании Nortel. В ее состав вошла система управления политиками Nortel Enterprise

Андрей Самсонов, руководитель группы сетевого проектирования Центра сетевых решений: *«При модернизации сетевой инфраструктуры мы всегда уделяем особое внимание плавному переводу информационных систем заказчика на новое решение. Чтобы достичь этого, еще на этапе проектирования необходимо не только скрупулезно продумать технические детали перевода, но и оценить риски и предложить способы их минимизации. Наличие плана проведения работ, во-первых, позволило Иркутскому заводу получить полное представление о действиях, которые будут проводиться, и сроках работ, а во-вторых, — обеспечить непрерывность функционирования информационных систем».*

Алексей Захаров, начальник бюро системно-технического обеспечения информационно-вычислительных сетей ИАЗ, руководитель проекта со стороны заказчика: *«Все изменения в сетевой инфраструктуре были заранее спланированы, проведен предварительный контроль оборудования и тестирование нового решения. Каждый участник команды проекта понимал, на каком этапе и что конкретно от него требуется. Благодаря такой организации работ удалось свести к минимуму число инцидентов, связанных со сбоями сети при реализации изменений».*

Policy Manager (EPM) v.4.3, управляющая приоритезацией трафика и параметрами безопасности сетевого доступа для бизнес-приложений.

При модернизации сети были созданы две серверные фермы, которые обеспечивают подключение информационных ресурсов основного и резервного центров обработки данных по технологии Gigabit Ethernet. Подключение серверных ферм к ядру выполнено с использованием технологий 10Gigabit Ethernet и SMLT. Применение технологии SMLT дает возможность осуществлять коммуникации между центрами обработки данных на втором уровне модели ISO OSI, что позволяет создавать распределенные кластерные комплексы.

Результат

В результате проекта была создана современная масштабируемая сетевая инфраструктура, обеспечивающая взаимодействие около 4500 пользователей.

Алексей Захаров, начальник бюро системно-технического обеспечения информационно-вычислительных сетей ИАЗ, руководитель проекта со стороны заказчика: *«Этот проект позволил нам повысить отказоустойчивость ЛВС и обеспечить развитие новых телекоммуникационных сервисов на базе IP-телефонии и ВКС за счет повышения качества сервиса передачи данных. В результате модернизации число сбоев в работе ядра и уровня распределения сети по вине сетевого оборудования приблизилось к нулю, т.к. теперь отсутствует единая точка отказа.*

Благодаря внедрению сетевой системы управления на базе продуктов Nortel ENMS и EPM сетевые администраторы всегда в курсе событий — узнают о сбоях первыми и оперативно устраняют неисправности. Практика реагирования на сбой по звонку пользователя уходит в прошлое. Повысилась управляемость сети, сетевые администраторы получили мощный инструмент управления сетевыми политиками. Теперь нет необходимости настраивать каждый коммутатор в отдельности, достаточно распространить политики для нужных устройств средствами Nortel EPM.

Пользователи ЛВС ИАЗ в свою очередь уже имели возможность почувствовать и оценить действие сетевых политик, запрещающих использование неразрешенного сетевого ПО и обеспечивающих повышение производительности бизнес-приложений.

В ходе выполнения работ мы нередко сталкивались с бдительными пользователями, привыкшими к тому, что появление сетевого администратора часто связано со сбоями сети и задававшими вопросы типа: «Что, опять сеть не работает? — или — «Нам выйти из сети?». Но чаще всего их опасения были напрасными. Проект выполнен в установленные сроки и в соответствии с установленными показателями качества. Использование активного сетевого оборудования нового поколения предоставляет возможность дальнейшего развития системы как с точки зрения внедрения новейших телекоммуникационных сервисов, таких, например, как унифицированные коммуникации, так и с позиции обеспечения меняющихся со временем требований защиты информации».

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Слободчикова Т.А. *(slobodchikova@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555