InformationSecurity

www.itsec.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ № 5, ноябрь 2014

Издание компании Groteck

10 ПРАВИЛ БЕЗОПАСНОСТИ СЕТИ

СПЕЦПРОЕКТ CYBER-WARFARE

КИБЕРРАЗВЕДКА

SECURITY INTELLIGENCE

РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ

Петр Ляпин, начальник службы информационной безопасности "НИИ Транснефть"

www.itsec.ru

powered by intersec

ТБ ФОРУМ®

Технологии Безопасности

10–12. 02.2015

КРОКУС ЭКСПО
ПАВИЛЬОН 2 | ЗАЛ 8

Видеонаблюдение ■ CCTV ■ IP–решения Интегрированные системы ■ Контроль доступа ■ Охрана периметра и ограждения ■ Охранно–пожарная сигнализация ■ Пожарная защита ■ Пожаротушение ■ Безопасность и охрана труда ■ Защита связи и информации ■ Биометрия ■ Спецтехника ■ Антитеррор ■ Охрана границ ■ Безопасность на транспорте

Организатор Groteck Business Media

БЕСПЛАТНАЯ РЕГИСТРАЦИЯ НА WWW.TBFORUM.RU

InfoSecurity Russia'2014:
новый уровень – лучший результат!

Наталья Рохмистрова,
директор выставки InfoSecurity Russia

С успехом прошла XI Международная выставка InfoSecurity Russia, подтвердив статус самого масштабного события отрасли.

Участники отмечают, что в этом году выставка вышла на новый уровень организации. Разноплановые деловые, технические и интерактивные мероприятия, проходящие в течение трех дней, позволили участникам и посетителям вести плодотворную совместную работу.

Руководители российских компаний и зарубежных представительств познакомились с самой полной экспозицией продуктов и услуг от лидирующих компаний отрасли для защиты информации. Экспозиция значительно расширилась за счет новых тематических кластеров и демо-зон, наглядно демонстрирующих все преимущества продуктов в действии.

Крупнейшее деловое событие рынка информационной безопасности и IT проходило в самых разнообразных форматах – пленарные и секционные заседания, круглые столы, практикумы, брифинги, семинары, конференции, симпозиумы – и объединило авторитетных экспертов, независимых аналитиков, представителей научной и бизнес-элиты.

InfoSecurity Russia уверенно занимает позиции рабочей площадки, на которой формируются инновационные проекты, актуальные для страны высокотехнологичные разработки превращаются в продуктовые решения и затем внедряются в важнейшие отрасли экономики. Представители регуляторов и государственных заказчиков ежегодно посещают выставку и активно следят за развитием InfoSecurity Russia и ее участников.

Подробный отчет о XI Международной выставке InfoSecurity Russia'2014 читайте на стр. 4.

Отзывы, мнения и впечатления читайте здесь: **www.infosecurityrussia.ru/2014/reviews.**

Благодарим всех участников и посетителей InfoSecurity Russia'2014 и приглашаем присоединиться к InfoSecurity Russia'2015!

XII юбилейная Международная выставка InfoSecurity Russia'2015

23–25 сентября 2015 г.
МВЦ "Крокус Экспо"

- Расширенная экспозиция.
- Живые демонстрации и тестирование оборудования.
- Самые актуальные темы и горячие дискуссии.
- Крупнейшие заказчики IT- и ИБ-решений.
- Больше российских и зарубежных гуру рынка.

Формируя программу и экспозицию 2015 г., мы объединяем положительный опыт и учитываем все пожелания посетителей и экспонентов, новые тренды и ситуации на рынке.

Экспертный совет уже начал работу по подготовке деловой программы в рамках выставки InfoSecurity Russia'2015. Выбраны предварительные темы и кластеры деловой программы. Подробный анонс посетители увидят уже в середине апреля 2015 г. Приглашаем специалистов и экспертов отрасли к формированию деловой программы и обсуждению наиболее актуальных тем.

До встречи в 2015 году!

Бронируйте участие в InfoSecurity Russia'2015 сейчас на лучших условиях!

По вопросам участия обращайтесь к Наталье Рохмистровой по тел.: (495) 647-0442 (доб. 2155); rohmistrova@groteck.ru.

По вопросам выступления в деловой программе обращайтесь к Екатерине Данилиной по тел. (495) 647-0442 (доб. 2270); danilina@groteck.ru

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СОДЕРЖАНИЕ

Журнал "Information Security/Информационная безопасность" № 5, 2014
Издание зарегистрировано в Минпечати России
Свидетельство о регистрации ПИ № 77-17607 от 9 марта 2004 г.

Учредитель и издатель
компания "Гротек"
Генеральный директор ООО "Гротек"
Андрей Мирошкин

СОДЕРЖАНИЕ

Издатель
Владимир Вараксин

Руководитель проекта
Наталья Рохмистрова,
rohmistrova@groteck.ru

Выпускающий редактор
Ольга Рытенкова, rytenkova@groteck.ru

Редактор
Екатерина Данилина, danilina@groteck.ru

Корректор
Ольга Михайлова

Дизайнеры-верстальщики
Анастасия Иванова, Ольга Пирадова

Фото на обложке
Алиса Урюпина

Группа управления заказами
Татьяна Мягкова

Юрисконсульт
Кирилл Сухов, lawyer@groteck.ru

Департамент продажи рекламы
Наталья Рохмистрова,
Ксения Чернобай

Рекламная служба
Тел.: (495) 647-0442,
rohmistrova@groteck.ru

Отпечатано в типографии
РА "Лидер", Россия
Тираж 10 000. Цена свободная

Оформление подписки
Тел.: (495) 647-0442, www.itsec.ru

Департамент по распространению
Тел.: (495) 647-0442,
факс: (495) 221-0864
Для почты 123007, Москва, а/я 82
E-mail groteck@groteck.ru
Web www.groteck.ru, www.itsec.ru

XI Международная выставка InfoSecurity Russia 2014. Итоги

6467	профессиональных посетителей
4378	специалистов посетили мероприятия деловой программы
187	мероприятий состоялось на стендах экспонентов, в конференц-залах и на главной сцене
226	российских и зарубежных участников InfoSecurity Russia'2014 представили на площадках InfoSecurity Russia самые передовые достижения, разработки и экспертизу в IT и ИБ-отрасли
136	докладчиков из числа ведущих мировых и российских экспертов представили свой профессиональный взгляд, оценку и прогнозы на развитие отрасли
18000	встреч экспонентов и докладчиков было зарегистрировано с аудиторией

infosecurity RUSSIA

24–26 сентября в Москве с успехом прошла XI Международная выставка InfoSecurity Russia'2014/ItSec by Groteck – самое масштабное событие рынка информационной безопасности России.

Церемония открытия

На торжественной церемонии открытия с пожеланием успехов и дальнейшего развития участникам и организаторам InfoSecurity Russia выступили: Шерстюк Владислав Петрович – советник секретаря СБ РФ, директор Института проблем информационной безопасности МГУ им. М.В. Ломоносова, Куц Анатолий Владимирович – заместитель директора ФСТЭК России, Мурашов Николай Николаевич – заместитель начальника Центра ФСБ России, Крылов Олег Вячеславович – начальник ГУБЗИ Банка России, Мирошников Борис Николаевич – член экспертного совета, руководитель комитета по информационной безопасности НП "Национальный платежный совет", Емельянов Геннадий Васильевич – Президент МОО "АЗИ", Шаклеин Дмитрий Иванович – член Экспертного совета комитета по безопасности и противодействию коррупции Государственной Думы ФС РФ, Вараксин Владимир Алексеевич – первый заместитель Генерального директора, "Гротек", Рохмистрова Наталья Борисовна – Директор выставки InfoSecurity Russia / ItSec by Groteck, "Гротек".

25 сентября выставку посетил Селин Владимир Викторович – директор ФСТЭК России.

В.В. Селин с делегацией осмотрел экспозицию выставки и ознакомился с решениями ведущих российских и зарубежных производителей.

25 сентября Захаров Виктор Николаевич – заместитель мэра Москвы в Правительстве Москвы по антитеррористической деятельности – также посетил InfoSecurity Russia'2014/ItSec by Groteck.

"Посещение выставки обусловлено тем, что на этой авторитетной и представительной площадке имеется возможность ознакомиться с современными разработками и подходами к решению вопросов обеспечения информационной безопасности как объектов ТЭК, так и в целом автоматизированных систем управления технологическими процессами, технологиями противодействия угрозам кибертерроризма", – отметил В.Н. Захаров, заместитель мэра Москвы в Правительстве Москвы по антитеррористической деятельности.

Благодарим партнеров и участников выставки

3M Россия, AirWatch by VMware, Akamai, Arbor Networks, BalaBit IT Security, Blue Coat Systems, Cezurity, Check Point Software Technologies, Codenomicon LTD, CyberArk, D-Link, Dell Sonic-

WALL, Diamond Security Group, Falcongaze, FEITIAN Technologies, Fluke Networks, GFI Software, Group-IB, HOB GmbH & Co. KG, HP, Imperva, INLINE Technologies, ISACA, IT Guard, IXIA, Juniper Networks, Kaspersky Lab, Landata Lieberman Software, McAfee, Part of Intel Security, Microsoft, Netwell, Nexetic, NVision Group, ONsec, Palo Alto Networks, Positive Technologies, R-Style, Radware, RQC, RRC, SearchInform, Setec, SoftpromStaffcop (ООО "Атом Безопасность"), STC Innovations, Synology Inc.TCC (Trusted Cloud Computers), Thales e-Security, VSS Monitoring, WALLIX, WD, Web Control, "Актив", АЛТЭКС-СОФТ, "АльтЭль", АМТ-ГРУП, Ассоциация защиты информации (АЗИ), "Астерос Информационная безопасность", "Безопасный Интернет", БЛАНК-КО, НПП "Гамма", "ДиалогНаука", ИВК (ЗАО "Информационная внедренческая компания"), "Инсайд РУС", ООО "Информзащита", учебный центр

"Информзащита", "Инфосистемы Джет", "ИнфоТеКС", КРИПТО-ПРО, "Монитор безопасности", Московский государственный университет приборостроения и информатики, МФИ Софт, НПО "РусБИТех", НПО "Эшелон", ОКБ САПР, РЕЛЭКС, ЗАО РНТ, "Русьтелетех", "С-Терра СиЭсПи", "СвязьКомплект", СКБ Контур, Фонд Сколково, "Судебные Технологии", "Трафика", "Тритфейс", АНКАД, Центр Специальной Системотехники, ЦИБИТ, ЭЛВИС-ПЛЮС, ОАО "Элкомсофт".

Благодарим Компанию "Лаборатория Касперского" за спонсорство зала С.

Благодарим компанию "Ландата" за спонсорство лент для бейджа.

Михаил Емельянников,
Управляющий партнер, консалтинговое агентство "Емельянников, Попова и партнеры"

Я считаю, что аналога этой выставки в России нет, это единственная отраслевая выставка с мощной деловой программой. Просто конференции, которые проходят и два, и три дня, не заменяют это мероприятие, потому что кроме конференции здесь есть возможность увидеть, попробовать, потрогать руками, поговорить со специалистами, а не только выслушать доклад одного маркетолога. Организаторы должны прилагать все усилия, чтобы она и дальше росла и развивалась.

Роман Кобцев,
директор департамента развития и маркетинга, ОАО "ЭЛВИС-ПЛЮС"

Мы каждый год участвуем в этой выставке. InfoSecurity Russia'2014 для нас стала особенной, потому что именно здесь мы выводим на рынок нашу новую технологию безопасности информации для мобильных платформ. Именно презентация новых продуктов – это то, что делает выставку выставкой и отличает ее от конференций и форумов. В этом году очень отрадно, что не только мы, но еще и ряд компаний представляет именно новые продукты.

Алексей Чирков,
Советник по правовым вопросам, Российский микрофинансовый центр

Благодарю команду InfoSecurity Russia за крайне высокий уровень организации и информационного наполнения программы выставки. Уверен, что участники по достоинству оценили уровень проведения мероприятия, по собственным наблюдениям, ощущается серьезное развитие по сравнению с предыдущим годом. Благодарю организаторов за возможность принять участие в выставке!

Алексей Ермаченков,
начальник отдела информационной безопасности, Банк "Кузнецкий Мост"

У InfoSecurity Russia нет аналогов: это лучшее многоформатное мероприятие с большим количеством стендов и докладов, посетителей и экспертов. Выставка может быть интересна специалисту с любым уровнем подготовки – как начального уровня, так и руководителю.

Павел Манык,
ведущий юрист, Юридическая компания "Зарцын и партнеры"

В целом выставка носит значимый характер как для компаний российского рынка, так и в части принимаемого сегодня законодательства. InfoSecurity Russia является связующим звеном, которое позволяет обобщить практику применения законодательства, а также актуализировать те вопросы, которые возникают у ряда компаний.

Евгений Акимов,
директор Центра информационной безопасности, R-Style

InfoSecurity Russia – это очень интересное мероприятие! Для меня это прежде всего площадка для подведения итогов, на которой эксперты по информационной безопасности и заказчики получают возможность обменяться мнениями о том, что получилось сделать в этом году. Мы участвуем не в первый раз, и качество выставки ежегодно растет.

Деловая программа

167 презентаций продуктов, инновационных разработок и достижений представили участники за 3 дня выставки на площадках и стендах InfoSecurity Russia'2014.

В рамках деловой программы InfoSecurity Russia'2014 прошло 19 конференций, участниками которых стали представители крупного пула производителей, потребителей и регуляторов.

- Защита АСУ ТП
- Кибербезопасность
- Противодействие мошенничеству
- Защита персональных данных
- Облачные технологии
- Импортозамещение: курс на независимость
- Карты: платежи, идентификация, мобильность
- Экономическая безопасность
- Firewalls: Next Generation
- ИБ-аутсорсинг – ближе, чем вы думаете
- DLP-эволюция
- ИБо-соки – ИБо-воды
- Наука и Безопасность
- Панельная дискуссия Фонда Сколково
- Взломать и защищать: от интернет-банка до электронного правительства
- ISACA
- Corporate Day, Industrial Day и Demo Day by Kaspersky Lab

Благодарим компании АМТ Груп, Монитор Безопасности, NVision Group, Jet InfoSystems, Kaspersky Lab, Positive Technologies, Фонд Сколково, Ассоциацию ISACA за спонсорство и оказанное содействие в организации мероприятий.

Благодарим российских и зарубежных докладчиков за успешные выступления, бесценный опыт, качественную экспертизу и профессиональный взгляд на развитие отрасли.

Демо-зоны

В соответствии с запросами заказчиков было организовано четыре тематические демо-зоны.

Внимание регуляторов и государственных заказчиков привлекла новая демо-зона "Сделано в России", где посетители смогли ознакомиться с передовыми технологиями отечественных производителей.

В новой демо-зоне "Инновации Сколково" компании-резиденты IT-центра "Сколково", специализирующиеся в сфере информационной безопасности, представили свои новейшие технологические решения и разработки.

В демо-зоне "Межсетевые экраны" посетители могли ознакомиться с экранами нового поколения и по заданному набору критериев выбрать подходящий МЭ для своей компании.

В демо-зоне "Экономическая безопасность" были представлены решения по криминалистике, защите коммерческой тайны, кадровой безопасности.

Интерактив на площадке

Благодарим компанию "Лаборатория Касперского" за представленную посетителям выставки игру IT-KARMA. Принять участие и проверить свои знания в области IT-безопасности смогли все желающие, а лучшие игроки получили ценные призы.

Одним из интерактивов для гостей InfoSecurity Russia стало знакомство с NFC-технологиями. На площадке прошла увлекательная игра, основанная на использовании NFC-карт. Посетители выставки узнали о возможностях NFC технологий и бесконтактной передаче данных, а также получили подарки от партнеров и организаторов. Благодарим компании VITEK, ISBC, INLINE Technologies, Инсайд РУС, ДиалогНаука, С-Терра СиЭсПи, ИнфоТеКС, IT Guard, Web Control за предоставленные призы и помощь в организации интерактива.

Благодарим спонсоров программы Pass Port – BalaBit IT Security, Информзащита, WALLIX, Synology Inc., WD, ОКБ САПР, – которые традиционно сделали счастливыми обладателями новых IPAD-Air трех участников конкурса.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Илья Медведовский,
генеральный директор, Digital Security

Для Digital Security выставка InfoSecurity Russia' 2014 – это прежде всего отличная конференционная программа. В этом году мы традиционно принимали участие в нескольких круглых столах, но я бы обратил особое внимание на секцию по безопасности АСУ ТП. По числу докладов, составу участников и количеству посетителей с этой секцией не сравнятся даже специализированные конференции по данной тематике, коих, кстати, у нас считанные единицы. Минимум маркетинга – максимум практики: регуляторы, хакеры-исследователи, вендоры, интеграторы – подобному составу выступающих можно было только позавидовать. Отличная конференция, которая была по достоинству оценена посетителями.

Организация и проведение служебных расследований

Петр Ляпин, *начальник службы информационной безопасности "НИИ Транснефть"*

Защита финансово-экономической стабильности компании от различного рода хакерских атак, как внешних, так и внутренних, является важной задачей для обеспечения стабильной работы любого бизнеса. Но если инцидент все же произошел, то необходимо правильно организовать и провести расследование внутри организации. О том, как это сделать, редакции журнала "Информационная безопасность/Information Security" рассказал начальник службы информационной безопасности ООО "НИИ ТНН" Петр Петрович Ляпин.

– Петр Петрович, расскажите, пожалуйста, какая на сегодня сложилась ситуация в России по киберпреступности?

– Достоверно ответить на этот вопрос практически невозможно. Официальную статистику всегда можно увидеть в отчетах МВД РФ "Состояние преступности в России", доступных на официальном сайте министерства*. Неофициальная, но порой более интересная информация представляется различными специализированными организациями. С учетом колоссальной латентности этого вида преступлений говорить о том, что официальные или неофициальные данные отражают реальное положение дел, по меньшей мере, неправильно. Это лишь малая часть окружающей нас действительности. Киберпреступность постоянно развивается, модифицируется вместе с изменением доступных и целевых технологий. Она всегда идет в ногу со временем.

– Системы, отвечающие за защиту и контроль информации, установленные в организациях, не могут дать 100% гарантии защиты от несанкционированных действий злоумышленников. Что же необходимо предпринять компаниям, если инцидент все же произошел?

– У каждого руководителя организации или ответственного лица должно быть четкое понимание, что необходимо делать в случае возникновения инцидента (что отключать, что проверять, куда сообщать и т.п.). При условии, конечно, что ставится цель предотвращать и пресекать такие инциденты. Причем речь не столько о четком плане и его безусловном соблюдении, а именно о понимании. А чтобы такое понимание отражало действительность, ответственному лицу необходимо знать, что должно защищаться, какими способами это осуществить и какие риски остаются. Иными словами, предварительная работа крайне необходима. А в случае возникновения инцидента – действовать согласно собственному плану (который может включать привлечение как сторонних экспертов, так и правоохранительных органов) либо максимально стабилизировать ситуацию и незамедлительно пригласить сторонних экспертов для определения необходимости и фиксации сведений (для будущей доказательной базы).

– Обозначьте, пожалуйста, основные этапы проведения служебного расследования киберпреступления.

– В первую очередь, необходимо помнить, что в соответствии с уголовным кодексом РФ преступлением признается виновно совершенное общественно опасное деяние. Служебные же расследования (правильнее – проверки), как правило, проводятся в рамках трудового и гражданского права. Если при проведении служебного расследования выявляются признаки преступления, (предусмотренного уголовным кодексом), то дальнейшим расследованием должны заниматься уполномоченные на то органы.

В большинстве случаев служебная проверка является первичной, поэтому крайне желательно заблаговременно обеспечить возможность сбора и фиксации информации в организации. Это могут быть как регистрационные журналы информационных систем, так и данные специализированных систем (например, класса DLP).

Порядок организации и проведения расследования преступлений детально регламентирован нормами УПК РФ. Что касается служебных проверок, то к их основным этапам следует отнести:

1) первичную фиксацию факта нарушения (служебная/докладная записка);

2) принятие решения о проведении служебной проверки (приказ);

3) первичное установление участников нарушения и получение объяснений;

4) сбор, фиксация дополнительных сведений (акты, протоколы);

5) обобщение сведений, установление виновных, определение нанесенного ущерба (акт проверки);

6) принятие решения о применении взыскания (приказ).

**http://mvd.ru/Deljatelnost/statistics/reports/*

В случае нанесения ущерба могут быть подготовлены документы для взыскания последнего уже в судебном порядке.

– Основная сложность, с которой сталкивается пострадавшая сторона, – сбор доказательств и их предъявление в судебном процессе, так как они могут быть легко изменены. Какие действия нужно предпринять организации, чтобы все данные попали в суд в первоначальном виде?

– Для ответа на вопрос необходимо четко зафиксировать определенные положения. В первую очередь, доказательства – это сведения (ст. 74 УПК РФ). Для получения доказательств необходимы:

1) надлежащий субъект (дознаватель, следователь, прокурор, суд);

2) надлежащая процедура (ст. 75 УПК РФ);

3) надлежащая форма (ст. 74 УПК РФ);

4) получение определенных видов доказательств возможно только в результате соответствующих следственных действий, предусмотренных УПК РФ.

Если речь идет о гражданском процессе, то по общему правилу каждая сторона должна доказывать те обстоятельства, на которые она ссылается. То есть каждая сторона убеждает в своей правоте суд любыми незапрещенными способами.

Если говорить об уголовном процессе, то организация может лишь собирать и представлять документы и предметы для приобщения их к делу в качестве доказательств.

Так, в зависимости от поставленных целей организация вправе использовать любые законные методы. В частности, для фиксации доказательств могут быть проведены соответствующие следственные действия, получены заключения экспертов и т.п.

– Случалось ли вам проводить подобные расследования или принимать в них участие?

– Конечно. Расследования именно преступлений имели место в основном в организациях финансового сектора, ввиду "популярности" различных видов кибермошенничества. В остальном – это по большей части служебные проверки (не уголовного характера).

– Петр Петрович, можете ли привести пример из практики?

– Свежими примерами поделиться не представляется возможным ввиду действующих обязательств.

Для одной очень распространенной системы ДБО был написан троян, собирающий ключевую информацию со всех машин, на которые он попадал. Кроме того, он обладал возможностью обеспечивать удаленное управление машиной жертвы с тем, чтобы использовать подключенный к ней аппаратный ключ, ее адрес, операционную систему и прочие идентификационные данные. Таким образом, злоумышленники переводили денежные средства со счетов клиентов – юридических лиц на карточные счета подставных физических лиц, с которых в течение 20–40 мин снимали эти деньги одновременно в десятке-двух банкоматов в трех соседних республиках.

– На ваш взгляд, какие секторы экономики наиболее уязвимы для хакерских атак?

– Правильнее говорить не об уязвимостях секторов экономики, а об уязвимостях эксплуатируемых систем вкупе с наличием и объемом интереса к ним со стороны злоумышленников. Так, в финансовом секторе интерес обусловлен возможностью организации относительно простых, но массовых мошеннических действий с картами и счетами. В предприятиях реального сектора экономики ситуация иная, так как преследуются другие интересы и ставятся другие цели. Если подходить со стороны статистики, то, например, касаемо финансового сектора доступно достаточно информации по мошенничеству в системах ДБО (отчасти ввиду массового характера некоторых преступлений), чего нельзя сказать, например, про сектор ТЭК. Но это вовсе не говорит о том, что наиболее уязвимым является финансовый сектор. Уязвимости присутствуют во всех системах. Их реализация определяется наличием интереса. Ну и не стоит забывать, что киберпреступления имеют высокую латентность в силу как объективных, так и субъективных причин. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Стратегический подход к трансформации

Александр Чижов, *управляющий партнер "Астерос Информационная безопасность"*

В конце 2012 г. группа "Астерос" объявила о принятии новой стратегии развития бизнеса, в рамках которой была сформирована компания "Астерос Информационная безопасность" (ранее бренд "КАБЕСТ"). Управляющим партнером новой бизнес-структуры был назначен Александр Чижов. На минувшей неделе редакция журнала "Information Security/Информационная безопасность" встретилась с Александром и побеседовала о произошедших за это время изменениях в бизнесе компании, специфике консалтинга в области ИБ и актуальных вопросах импортозамещения на рынке информационной безопасности.

– Александр, позапрошлой весной вы были назначены главой "Астерос Информационная безопасность". Давайте сравним компанию образца 2011–2012 гг. и ваш сегодняшний бизнес. Какие стратегические изменения произошли за это время?

– К моменту моего назначения компания "Астерос Информационная безопасность" вплотную подошла к необходимости преобразований основных бизнес-процессов. Заметное повышение уровня зрелости рынка и, как следствие, желание клиентов решать действительно серьезные проблемы в области обеспечения защиты информации при минимальных финансовых затратах ставили перед нами задачу диверсификации бизнеса. Было очевидно, что изменения в компании должны были коснуться буквально всех направлений: стратегического, управленческого, операционного и проектного. Основная ставка была сделана на разработку и внедрение нового подхода к реализации проектов, а именно – усиление в них консалтинговой составляющей. Для совершенствования управления была изменена структура компании, подразумевающая создание тесно взаимосвязанных между собой, но финансово автономных практик. Также был создан единый центр технической поддержки.

В целях реализации нового подхода мы существенно переработали продуктовый портфель, дополнив его новыми предложениями, в том числе, в области консалтинга. Это позволило нам предлагать рынку продукты, востребованные сейчас и при этом учитывающие перспективные направления развития в области защиты информации. Большой объем работы был проделан по анализу рынка и выявлению потребностей существующих и потенциальных клиентов. Параллельно мы усилили команду "Астерос ИБ" и продолжаем это делать за счет привлечения новых сотрудников. Сейчас я могу с уверенностью сказать, что мы справились с решением задачи трансформации компании. Нам удалось сохранить сильные позиции у ключевых клиентов, которые поддержали новый подход к оказанию услуг в области ИБ.

– Вы пришли на рынок информационной безопасности из консалтинга. Насколько теперь рынок ИБ в целом близок вам?

– Безусловно, нелегко адаптироваться в отрасли, которая достаточно продолжительное время жила на навязанном спросе, в консалтинге такое сложно встретить. Приходя в лидирующую компанию на рынке ИБ, мне важно было сохранить ее позиции и создать фундамент для обеспечения дальнейшего роста в условиях изменяющегося рынка. Не скрою – это было непросто. Кто-то не согласился с моими идеями и выбрал смену места работы, а кто-то, наоборот, поддержал и продолжает поддерживать. Именно благодаря сильной команде я смог освоить новое для себя направление бизнеса и продолжаю развивать полученные знания, накапливать необходимый опыт.

– Хотелось бы поднять вопрос о том, какие ключевые практики, компетенции у компании есть сегодня? На какие направления бизнеса вы делаете основные ставки? За счет чего планируете развивать бизнес?

– Перейдя к модели управления по практикам, мы выделили для себя ключевые направления в области ИБ. Среди них сегодня: аудит и консалтинг, аналитические и инфраструктурные решения, системы идентификации и контроля доступа к IT-ресурсам, техническая защита информации.

У каждой практики есть свое рыночное предложение, в основе которого лежит анализ конкурентной среды, актуальные тренды и имеющаяся отраслевая и продуктовая экспертизы. При формировании продуктового портфеля практик мы старались сбалансировать его таким образом, чтобы удовлетворить потребности наших клиентов сегодня и попытаться заглянуть даже не в завтра, а чуть дальше, и ответить на вызовы, которые их ждут в будущем.

Основными направлениями деятельности в области аудита и консалтинга являются разработка стратегии ИБ, организационно-распорядительной документации по обеспечению ИБ (включая концепцию, политики, процедуры и стандарты в области информационной безопасности, методические материалы), аудит или оценка соответствия требованиям ИБ, разработка электронных авторских курсов для дистанционного обучения ИБ, аттестация объектов информатизации и аутсорсинг.

Также в нашем фокусе – построение процесса автоматизации управления рисками ИБ. Кроме того, мы видим большие перспективы в такой сфере, как управление инцидентами и опе-

ративное управление ИБ. Не менее востребованным сегодня является направление визуальной аналитики для решения задач экономической и информационной безопасности, а также для выявления фрода.

Я бы отметил большой шаг вперед, который мы сделали и в части комплексных решений по управлению доступом к IT-ресурсам (IAM, Identity Governance): обновлена наша методологическая и техническая составляющие реализации проектов по управлению доступом. Мы постоянно совершенствуем статистические и аналитические подходы к построению ролевой модели доступов, которую мы одними из первых на российском рынке внедрили у наших клиентов. Мы уделяем пристальное внимание ее развитию и считаем одним из основных компонентов успешного и эффективного внедрения IAM-решения.

В области инфраструктурных решений актуальными направлениями являются автоматизированный анализ программного кода, контроль действий администратора, противодействие целенаправленным атакам (Advanced Persistent Threat – APT). Также все большим спросом у наших клиентов пользуется аутсорсинговая модель предоставления услуг.

Иными словами, нам интересно множество направлений ИБ, никаких ограничений для горизонтального роста компании у нас нет. Развитие бизнеса мы планируем, прежде всего, за счет увеличения как продуктовых специализаций в практиках, так и выделения новых практик для фокусирования на определенном направлении ИБ.

– В чем преимущество вашего, будем его называть, "консалтингового подхода" к ИБ-проектам?

– Сегодня на рынке ИБ превалирует технический аспект реализации проектов. На мой взгляд, разработке процессной составляющей практически никто не уделяет должного внимания. Мы придерживаемся других принципов. Прежде всего, нам важен результат, который измеряется в показателях, понятных бизнесу, и соответствует его приоритетам и ожиданиям от ИБ. Мы не пытаемся прикрыть бреши: в основе нашего подхода – долгосрочная стратегия развития ИБ, созданная в результате "глубокого погружения" в специфику бизнеса клиента.

Что делаем мы? Во-первых, помимо службы ИБ и IT-подразделения, мы вовлекаем в реализацию проекта всех лиц, причастных к работе с конфиденциальной информацией в организации. Они также участвуют в реализации ИБ-проекта, и нам важно, чтобы они хорошо понимали и разделяли наш подход к управлению ИБ в компании. Во-вторых, это, безусловно, обучение и регулярное информирование. И в-третьих, это оценка зрелости процесса после его внедрения, в том числе разработка программы по повышению его уровня зрелости. Подход "внедрил и забыл" – это не к нам. Взять хотя бы проект по интеграции DLP. Для того чтобы создать эффективно работающую систему DLP, вокруг самого технологического "ядра" проекта нужно выстроить процессы работы с конфиденциальной информацией на всех уровнях, имеющих к ней отношение. Постановку данных процессов мы реализуем в наших проектах.

– Не могу не упомянуть о том, что на рынке ходили слухи об оттоке персонала из "Астерос ИБ" в связи с уходом прежнего лидера компании. Насколько они правдивы? Как изменилась численность штата? Каков процент ротации?

– Как я уже говорил, на момент моего назначения было важно сохранить экспертизу в лице ключевых сотрудников и сформировать команду, готовую работать по новым правилам. Сегодня можно с уверенностью сказать, что "Астерос ИБ" – это команда сильных профессионалов, способная решать нетривиальные задачи в области ИБ.

Вы упомянули об оттоке персонала. Действительно, в первые месяцы компанию покинуло существенное количество персонала, и по некоторым направлениям приходилось практически заново собирать экспертов, но должен сказать, что задача была решена в кратчайшие сроки, и мы смогли пройти этот период с минимальными потерями, не только сохранив ключевых клиентов, но и приобрели новых.

В результате реорганизации и оптимизации ряда ключевых бизнес-процессов нам удалось, не увеличивая штат сотрудников, повысить качество реализации проектов. В области управления персоналом и его мотивации была проделана большая работа. На мой взгляд, люди в нашем бизнесе – это основной залог успеха деятельности. А сотрудники, целиком и полностью разделяющие основные ценности работы компании, – двойной успех.

– Какие результаты работы "Астерос ИБ" в отраслевом разрезе вы бы назвали наиболее значимыми за прошедшие полтора года?

– Каждая практика добилась за прошедшие полтора года значимых результатов. Из основных успехов могу отметить расширение бизнеса в финансовой и телекоммуникационной сферах, развитие взаимодействия с крупными государственными организациями и коммерческим сектором.

– На повестке дня в последнее время регулярно звучит тема импортозамещения. В связи с этим планируете ли вы развивать отношение с азиатскими поставщиками? Как в целом может измениться ваш вендорский портфель на фоне текущей экономической и политической ситуации?

– В настоящее время мы активно ведем переговоры как с российскими производителями программных и аппаратных средств защиты информации, в том числе реализуемых на основе отечественного общего и прикладного ПО и элементной базы. Также мы взаимодействуем с представителями белорусских, казахстанских, китайских и израильских компаний, занимающихся вопросами создания средств защиты информации и не привязанных к санкционным действиям США и Евросоюза.

Одно из наших преимуществ на рынке ИБ заключается в вендоронезависимости. У нас прекрасные партнерские отношения практически со всеми крупными производителями средств защиты информации и их дистрибуторами. Поэтому мы имеем возможность предлагать клиентам наиболее приемлемые для них решения исходя из критерия "цена-эффективность", включая и стоимость их последующей эксплуатации. ●

Кибервойны будущего – к чему готовиться законодателям и корпорациям

Игорь Башелханов, *заведующий лабораторией, преподаватель, ФГОБУ ВПО Финансовый университет при Правительстве Российской Федерации, к.ф.-м.н.*

Термин “кибервойна” мы связываем с термином “кибернетика” (“наука об управлении”, “управление и связь с животным и машиной” – по Н. Винеру, 1948 г.), а также с понятием “цифра” (обратите внимание на написание слов “cyber” и устаревшего – “цифирь”, еще петровского времени). Поэтому нужно смотреть на проблему кибервойн более широко, чем это принято. Что это значит? Классическая война – это “горячая война” с использованием материального оружия и энергии, которая до поры до времени упрятана в материи (атомное оружие и т.п.). Действующими компонентами такой войны являются материя и освобожденная из нее энергия.

Начнем с дефиниций

Кибервойна – это массированная обезличенная генерация хаоса в социотехнической системе, связанная с совместным применением программируемых технических средств и программируемых социальных элементов (биоисполнителей, биороботов). Программа (последовательность команд) – это идеальное оружие (прежде всего, в философском смысле – вспомним материалистическое и идеалистическое течения в философии). Это оружие идеально и в обычном смысле: на первых порах оно не приводит к летальным последствиям для людей, оно невидимо, не оставляет материальных следов, а если следы и остались – легко уничтожаются. Рука об руку с программированием идут математика и информационная безопасность (где цифра – там и математика, а за ней видна криптография). На данном этапе развития технологий можно говорить о гибридном социотехническом оружии. Речь идет об использовании в кибервойне не только ИКТ, но и исполнителей – людей (так называемых "животных", по терминологии "отца кибернетики") – и исполнительных устройств – машин. Промежуточной целью любых войн является создание хаоса (разрушение старых связей и отношений, в особенности – образовательных, политических, экономических), которое дает возможность в конечном счете переключить источники энергии-информации поражен-

Первая мировая война была, образно говоря, войной прикладных химиков, Вторая мировая война – войной прикладных физиков, третья мировая война станет войной математических физиков и прикладных математиков.

Кибервойна – это массированная обезличенная генерация хаоса в социотехнической системе, связанная с совместным применением программируемых технических средств и программируемых социальных элементов (биоисполнителей, биороботов). Программа (последовательность команд) – это идеальное оружие

ной социотехнической системы на нового бенефициара, выгодоприобретателя. Финансово-экономическими признаками начала кибервойны можно назвать замедление роста, остановку, а затем падение валового внутреннего продукта (ВВП) страны-жертвы условно более чем на один процент за один месяц.

Теория динамического хаоса

Теории хаоса, точнее, динамического хаоса, были развиты французским физиком, философом Анри Пуанкаре, советскими математиками-академиками А.Н. Колмогоровым, В.И. Арнольдом и немецким математиком Ю.К. Мозером (КАМ-теория). Приложил свой ум к его развитию и физикохимик русского происхождения Илья Пригожин – нобелевский лауреат, автор "Философии нестабильности". Американскими химиком Джорджем Коуэном и физиком Мюрреем Гелл-Манном был создан в 1984 г. Институт сложности в Санта-Фе (SFI). В дальнейшем над этими проблемами работали советский и российский академик А.А. Самарский, член-корреспондент РАН С.П. Курдюмов и продолжает работать профессор Г.Г. Малинецкий и их партнеры. Поскольку вышеперечисленные ученые знали механизмы зарождения и эволюции хаоса, то они могли предложить "противоядие", "противооружие". Наиболее четко видевшим гуманитарные проблемы, проистекающие из реалий и планов математической войны, был академик В.И. Арнольд [1]. Приведем цитату из речи В.И. Арнольда на парламентских слушаниях 2002 г., эмоционально изображающую план поражения в этой войне: "Этот план производит общее впечатление плана подготовки рабов, обслуживающих сырьевой придаток господствующих хозяев: этих рабов учат разве что основам языка хозяев, чтобы они могли понимать приказы". Вот другие слова, приписываемые Арнольду: "Вот почему бурбакистская мафия, заменяющая понимание науки формальными манипуляциями с непонятными "коммутативными" объектами, так сильна во Франции, и вот что угрожает и нам в России". Разъясняя это, математик приводит пример: "Французский школьник-отличник на вопрос: "Сколько будет два плюс три?" отвечает: "Три плюс два, так как сложение коммутативно", а считать до пяти, хотя бы на пальцах, его не научили (видимо, вследствие "компьютерной дидактики")". "Физико-математический абсолют" и злоумышленники создают так называемый "управляемый хаос" во всех сферах жизни поражаемого общества, зачастую интуитивно (невольно, подсознательно) используя теорию динамического хаоса.

Математические войны

Поскольку войны могут длиться десятилетиями, для "физико-математического абсолюта" или для злоумышленных выгодоприобретателей очевидно,

что наиболее эффективным способом является математическое, программное поражение детей и молодежи. Через такую математико-"артиллерийскую" подготовку первоначально прошли французские и американские молодые люди, а затем европейские и украинские учащиеся и студенты. Понятие о "математических войнах" появилось в США в конце 80-х – начале 90-х гг. XX в. и отражает уровень накала страстей по проблемам школьной математики. В Европе подобные войны коррелируют с "болонским процессом". Начало "математико-цифровым войнам" положила публикация в 1989 г. нового стандарта школьного математического образования, подготовленного Национальным советом учителей математики США (National Council of Teachers of Mathematics, NCTM). Результатом почти двадцатилетних математических войн стал мировой кризис 2008 г., наступивший из-за деградации и хаоса в головах американской и европейской молодежи, а также молодежи других частей планеты, которая в свое время вольно или невольно клюнула на программную удочку и которая за это время стала элитой политики, бизнеса и других сфер.

Заключение

Будущая "идеальная кибервойна" будет включать не только применение нормативно-право-конституционных (НПК), организационно-экономико-маркетинговых методов (ОЭМ) поражения противника, но и применение непосредственно физико-технико-математического оружия (ФТМ), но уже в полном объеме [2]. Первые две группы мер также уже сейчас имеют явные или неявные математические признаки. В настоящее время "обкатывается" часть элементов этой войны в виде взаимных экономико-политических санкций – самоотказов в обслуживании (DoS и DDoS-самоатаковывание) – ущербное не только для технических, но и для социальных подсистем. Вспомним также использование термина "перезагрузка" президентом США Б. Обамой. Таким образом, компьютерный подход распространяется на социально-государственные отношения. Соответственно, НПК (оружию должны противопоставляться

НПК) – меры защиты. Нормативы – это стандарты, инструкции, политики безопасности. Для того, чтобы отсечь "раковые опухоли", последствия перерождения собственных элементов, инсайдеров (перепрограммирования нейронных клеток и в целом людей) во время будущей кибервойны, нужно установить собственные стандарты, нормативы, политики безопасности, нужно создавать, сохранять и развивать свои языки, в том числе и языки программирования, создавать свои операционные системы и т.п., не распространяя их по всему миру, поскольку при их совместимости очень вероятными становятся вирусные пандемии (как в случае, например, с вирусом Эбола), но уже в виртуальном пространстве. Аутентичные, этнические, национальные стандарты должны быть обязательны для исполнения. В правовом поле, регулирующем ИКТ и информационное право, органам нужно устанавливать цифровое правосудие, работающее уже в наносекундном режиме и во всем цифровом пространстве. Поэтому на международном уровне должен быть введен Цифровой кодекс. Нужно устанавливать пределы гонки цифровых вооружений путем заключения международных договоров.

Корпорациям, во-первых, важно иметь в виду, что качество и количество DoS- и DDoS-атак и других инцидентов информационной безопасности подчиняется математическим закономерностям, а также что они определяются на 70–80% непосредственно уязвимостями человека, человеческим фактором. Во-вторых, с маркетинговой точки зрения нужно срочно обратить внимание на способность их цифро-программных устройств различного назначения обеспечивать информационную безопасность. В-третьих, производителям и потребителям надо знать, что в 2006 г. исследовательская группа из Лос-Аламосской национальной лаборатории (США) впервые произвела передачу секретной информации на расстояние больше чем 100 км, используя принцип квантовой криптографии, теоретически обеспечивающей абсолютную тайну переданного сообщения. Дальнейшее, уже засекреченное, развитие этой отрасли приведет к бессмысленности DLP, BYOD, к краху и смерти классической математической криптографии и современных программно-аппаратных средств защиты информации. Квантовый компьютер, устроенный на физических принципах квантовой механики, легко может взломать шифр RSA, алгоритм DES, стандарт RC5 и т.п., и, таким образом, самая секретная и конфиденциальная информация, возможно, уже завтра станет явной – тайна исчезнет.

Литература

1. Арнольд В.И. Что такое математика? – М.: МНЦМО, 2012. – 108 с.

2. Башелханов И.В., Башелханов С.И. Концепция защиты информации. Новые аспекты обеспечения информационной безопасности // VI Международная научно-практическая конференция студентов, аспирантов и молодых ученых "Информационные технологии в науке, бизнесе и образовании (Технологии безопасности)". – М.: Изд-во Финуниверситета. – 2013. – С. 35–38

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Будущая "идеальная кибервойна" будет включать не только применение нормативно-право-конституционных, организационно-экономико-маркетинговых методов поражения противника, но и применение непосредственно физико-технико-математического оружия, но уже в полном объеме.

Квантовый компьютер, устроенный на физических принципах квантовой механики, легко может взломать шифр RSA, алгоритм DES, стандарт RC5 и т.п., и, таким образом, самая секретная и конфиденциальная информация, возможно, уже завтра станет явной – тайна исчезнет.

Лучшие практики противодействия киберугрозам

Дмитрий Волков, *руководитель направления предотвращения и расследования инцидентов информационной безопасности, Group-IB*

Все уже давно осознают, что злоумышленники всегда на шаг впереди. Они диктуют правила, а производители средств защиты им следуют и постоянно пытаются догнать. Сам подход к противодействию киберугрозам не изменился — он носит четко оборонительный характер. В некоторых случаях люди защищаются от того, о чем имеют крайне поверхностное понимание. Все знают, что есть киберпреступники и они используют уязвимости, вредоносные программы, что есть целевые атаки, но лишь очень маленький процент специалистов по ИБ знает, как эти уязвимости эксплуатируются, почему все известные уже несколько лет вредоносные программы по-прежнему не детектируются средствами антивирусной защиты, как именно проходят целевые атаки, почему злоумышленникам удается попасть в жестко изолированные сегменты сети и т.д.

Cyber Intelligence позволяет собрать сведения о том:
- какие атаки уже произошли или могут произойти;
- как действия атакующего могут быть распознаны и обнаружены;
- как эти действия могут быть смягчены;
- кто стоит за этими атаками;
- каковы мотивы атакующих и чего они пытаются добиться;
- каковы их возможности с точки зрения тактики, техники, процедур, используемых ими ранее и в скором будущем;
- какие уязвимости, ошибки конфигурации они эксплуатируют;
- какие действия они предпринимали в прошлом, и т.д.

Незнание деталей приводит к тому, что при разработке стратегии противодействия киберугрозам, оценке рисков и закупках средств защиты часто принимаются неверные решения. Практически полностью отсутствуют данные о том, сколько и каких атак было вчера, какие новые угрозы появились, как злоумышленники действуют в определенных ситуациях. Им невозможно противостоять вслепую. Эту ситуацию можно сравнить с тем, как вести войну без данных о количестве и дислокации врага, используемом им вооружении, источниках подкреплений и т.п. Именно это является одной из основных причин, почему злоумышленники настолько успешны в своих действиях и почему увеличение бюджетов на ИБ не приводит к снижению уровня киберпреступности.

Осознание этой проблемы привело к появлению такого направления у частных компаний, как Cyber Intelligence. В своей статье я буду использовать именно англоязычный термин, поскольку его русский перевод – киберразведка – вызывает у людей ложное ощущение, связанное со взломами и шпионажем. На самом деле это не так. Забегая немного вперед, скажу, что многие вендоры средств защиты подхватили эту тенденцию и начали заявлять о том, что они теперь тоже предоставляют такую услугу, однако на практике все сводится к тому, что вместо Cyber Intelligence вам дают черные списки IP-адресов, доменных имен, хеши файлов. Такое "нововведение" не имеет никакого отношения к реальной Cyber Intelligence. Как и в обычной разведке, выясняющей, какие у атакующего возможности, намерения и текущие действия, Cyber Intelligence добывает сведения о том:
- какие атаки уже произошли или могут произойти;
- как действия атакующего могут быть распознаны и обнаружены;
- как эти действия могут быть смягчены;
- кто стоит за этими атаками;
- каковы мотивы атакующих и чего они пытаются добиться;
- каковы их возможности с точки зрения тактики, техники, процедур, используемых ими ранее и в скором будущем;
- какие уязвимости, ошибки конфигурации они эксплуатируют;
- какие действия они предпринимали в прошлом, и т.д.

Хороша реакция вовремя

Лучшая практика противодействия киберугрозам – это сочетание знаний, полученных от Cyber Intelligence, и уже внедренных средств защиты. Но такие знания имеют значения, только если они получены оперативно. Сейчас же о чем-то новом узнают с недопустимыми задержками из аналитических отчетов или какой-то новости, просочившейся в СМИ, и, как всегда, очень многое остается неосвещенным. Приведу пример.

Пример

Было обнаружено, что одна из преступных групп начала проводить целевые атаки на банки. То есть их целью является получение доступа к банковским системам, которые позволят злоумышленникам перевести несколько сотен млн руб. (только за 1 год насчитывается более 36 случаев). Чтобы остановить злоумышленников до момента получения доступа в сеть банка или уже после того, как они этот доступ получили, банкам необходимо предоставить сведения о том, как эта преступная группа работает, и индикаторы, по которым можно определить действия данной преступной группы во время атаки. К таким индикаторам могут относиться:
- текст письма, рассылаемого злоумышленниками;
- адрес отправителя;
- номера телефонов, с которых они "прозванивают" банки;
- IP-адреса серверов, на которые их вредоносные программы передают данные;
- легальные инструменты,

Для эффективного противодействия киберугрозам необходимо точно знать своего врага и как он действует. Источником такой информации может быть Cyber Intelligence, использование которой поможет службам безопасности получать сведения о самых актуальных угрозах, что улучшит их ситуационную осведомленность, поможет в выработке мер защиты и принятия верных оперативных и стратегических решений.

которые используются злоумышленниками для изучения внутренней инфраструктуры банка, и т.д.

Если такая информация будет предоставлена через месяц после обнаружения, то, скорее всего, злоумышленники уже успеют значительно закрепиться в сети банка или даже украсть деньги, за которыми они пришли. Если по индикаторам скомпрометированные банки не смогли найти следов работы злоумышленников (бывает и такое), то можно исследовать серверы, используемые злоумышленниками, и дать точные адреса банков и названия компьютеров и серверов, которые уже находятся под контролем этой преступной группы.

Эффективное противодействие киберугрозам

Cyber Intelligence – крайне полезный инструмент для эффективного противодействия киберугрозам, но основной проблемой является именно получение значимой информации. Например, в компаниях вроде Google, Facebook, City Group, HSBC существуют целые подразделения с сотнями людей, которые занимаются изучением киберугроз. Но гиганты, работающие по всему миру, могут позволить себе такое подразделение, а компаниям поменьше это недоступно. Специалистов очень мало, и чтобы они эффективно работали, им нужно предоставить соответствующую инфраструктуру мониторинга, постоянно погружаться в разбор самых разных инцидентов.

Подводя итог

Реагировать на инцидент после того, как он уже произошел, очень дорого как с точки зрения управления последствиями, так и для искоренения атакующего из внутренней инфраструктуры. Для того, чтобы стать проактивным, необходимо останавливать продвижение злоумышленника еще до этапа эксплуатации и получения контроля над системами.

Подводя итог, еще раз подчеркну, что для эффективного противодействия киберугрозам необходимо точно знать своего врага и как он действует. Источником такой информации может быть Cyber Intelligence, использование которой поможет службам безопасности получать сведения о самых актуальных угрозах, что улучшит их ситуационную осведомленность, поможет в выработке мер защиты и принятия верных оперативных и стратегических решений. ●

Колонка эксперта

Петр Ляпин,
начальник службы информационной безопасности, "НИИ Транснефть"

Преступления

Что такое киберпреступление? С одной стороны, это преступление, имеющее специальный состав, как, например, "неправомерный доступ к компьютерной информации" или "создание, использование и распространение вредоносных компьютерных программ". С другой стороны, это преступление с классическим составом, но совершаемое с помощью ИКТ, как, например, "мошенничество". Сложности, связанные с транснациональностью киберпреступлений, указывают на необходимость унификации составов по возможности во всех странах мира. Нельзя привлекать к ответственности лицо за деяние, которое на территории государства его текущего пребывания преступлением не является, даже если другое заинтересованное государство содержит в своем уголовном законе необходимые составы. Реализация ответственности в таком случае станет возможной лишь при нахождении лица под юрисдикцией соответствующего государства.

Сразу вспоминается история с пребыванием основателя сайта WikiLeaks Джулиана Ассанжа в посольстве Эквадора в Лондоне (где он находится с середины 2012 г.).

Решение задачи унификации уголовного законодательства заключается в разработке и принятии общеобязательного международного акта, содержащего единую терминологию и составы киберпреступлений, которые затем будут включены в национальные уголовные законы.

В 2010 г. по инициативе Генеральной Ассамблеи ООН (резолюция 65/230) Комиссией UNODC была создана межправительственная группа экспертов для всестороннего исследования проблемы киберпреступности, в результате которого были выделены 14 составов киберпреступлений: незаконный доступ к компьютерной системе; незаконный доступ, перехват или получение компьютерных данных; незаконное вмешательство в данные или в систему; производство, распространение или хранение средств неправомерного использования компьютеров; нарушение конфиденциальности или мер защиты данных; компьютерное мошенничество или подлог; компьютерные преступления, связанные с использованием личных данных; компьютерные преступления, касающиеся авторских прав и товарных знаков; компьютерные преступления, связанные с причинением личного вреда; компьютерные преступления, связанные с расизмом или ксенофобией; использование компьютера с целью производства, распространения или хранения детской порнографии; использование компьютера для завлечения или "груминга" детей; использование компьютера для содействия террористическим преступлениям.

Следует отметить, что большинство из них нашли свое отражение в УК РФ. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Лучшие практики противодействия DDoS-атакам

Александр Лямин, *руководитель Qrator Labs*

DDoS-атаки (от английского Distributed Denial of Service, или "Распределенный отказ в обслуживании") не являются новинкой в сфере киберпреступлений: их изобрели далеко не вчера, и такой вид атак уже стал довольно острой проблемой для многих компаний. DDoS приобретает все более разрушительный характер, становясь эффективным инструментом для нанесения экономического ущерба и репутационного урона и небольшим интернет-магазинам, и крупным корпорациям, и ведущим СМИ.

С каждым годом технологии вывода Web-сайтов из строя становятся все доступнее, и это неудивительно: способы генерации большого количества трафика всем известны, а стоимость проведения атак не так уж велика. В то же время растет и обеспокоенность бизнеса проблемой DDoS, и уже многие компании стараются быть готовыми к атакам заблаговременно. На сегодняшний день выработаны определенные практики по защите от подобных угроз, позволяющие предотвратить опасность, а не разбираться с ее последствиями. Но в первую очередь необходимо понять, какие проблемы для бизнеса несет в себе DDoS, и затем говорить о том, как их можно решить.

Модель угроз

В составлении модели угроз существуют два основных подхода. Первый – формирование списка актуальных на сегодняшний день атак.

Общий список угроз является суммарным результатом непрерывных исследований всех игроков индустрии безопасности. Часть этих атак учитывает при выпуске своего оборудования вендор, и далее заказчик составляет для себя модель угроз, выбирая решение, которое сможет по этой модели защитить его инфраструктуру (что приводит к значительному сокращению перечня возможных атак). Однако даже изначальный список является полным лишь на текущий момент, и буквально завтра он может дополниться новыми угрозами. Соответственно, в соглашении на использование оборудования обычно прописывается, что производитель не гарантирует нейтрализации атаки, если она не входит в обозначенный перечень. При этом современные инструменты DDoS постоянно развиваются, и, например, таргетированные атаки гарантированно не попадут в такой список и смогут обойти защиту оборудования.

Второй подход заключается в том, что заказчику гарантируется доступность его приложения извне с определенным SLA (соглашением об уровне предоставления услуг) вне зависимости от того, какие атаки могут случиться. В этом случае DDoS-атаки классифицируются, исходя из сетевой модели OSI: они могут производиться на канал, конечный автомат TCP или приложение. То есть атакующая сторона может или "забивать" каналы дата-центра/сервера/провайдера, или исчерпывать ресурсы операционной системы, например, открывая большое число соединений, или эксплуатировать слабые места Web-приложения.

Маршрутизация

Отдельно стоит отметить проблемы маршрутизации (протокол BGP, отвечающий за глобальную доступность сетей в Интернете). При помощи атак route leak злоумышленник может попытаться незаметно увести трафик на себя с целью его прослушивания. Безусловно, прослушивание не приводит к отказу в обслуживании, но во время DDoS-атаки, когда информационные ресурсы жертвы недоступны, атакующая сторона может создать поддельный ресурс взамен атакованного, что гораздо опаснее, чем просто просмотр чужого трафика. Во II квартале 2014 г. зарегистрировано 4153 подобных инцидента с маршрутизацией, из них 608 – с влиянием на внутрироссийский трафик.

Доступность

Популярность DDoS-атак объясняется низкой ценой: вывести из строя сайт конкурента дешевле, чем продвигать свой, а если атака реализована в период рекламной кампании у "жертвы", то к стоимости простоя онлайновой части бизнеса можно прибавить маркетинговый бюджет. Для осуществления "заливки" канала паразитным трафиком атакующей стороне потребуется один или два сервера в хостинге, который не реагирует или очень медленно реагирует на жалобы и старается не сотрудничать с правоохранительными органами (bulletproof hosting service), – это $50–70 в месяц за сервер с гигабитным подключением и список амплификаторов*, который можно купить на черном рынке или собрать самому за 2–3 часа.

В таблицах 1 и 2 приводится актуальная статистика по числу уязвимых серверов, которые могут выступать в качестве амплификаторов, в разбивке по типам. Сегодня амплификаторов так много, что технически нет проблемы организовать атаку на канал в несколько сотен гигабит.

Атаки на TCP несколько сложнее и дороже, так как для

*Под амплификатором понимается UDP-сервер, работающий без авторизации, который на небольшой запрос способен посылать в разы больший ответ. Для его использования злоумышленник подделывает адрес отправителя UDP-пакета, подставляя адрес атакуемого сервиса. В результате хакер посылает небольшие пакеты, не очень нагружая свои каналы, а амплификатор отвечает в разы большими в адрес атакуемого сервиса.

них необходимо арендовать ботнет. Атака же на само приложение всегда таргетирована: атакующая сторона выбирает ту часть, которая нагружает сервер больше всего, например поиск по сайту, и генерирует для этого функционала большое количество запросов при помощи ботов. На сегодняшний день была зарегистрирована самая большая атака с участием более 450 000 ботов, которые работали как полнофункциональный браузер и пытались имитировать поведение на сайте живого человека.

Решение проблемы. Лучшие практики

Защищаться от DDoS-атак можно по-разному. Первый способ, к которому обычно прибегают вначале, – это организация самостоятельной защиты, но подобный вид мер безопасности способен нейтрализовать лишь самые простые атаки: установка front-end Nginx, запрет протоколов ICMP и UDP могут значительно облегчить жизнь сервису, но только до определенного уровня.

Также защиту может предоставлять хостинг-провайдер или оператор связи, но их возможности ограничены доступным для них каналом, и ни один, ни другой не будут разбирать высокоуровневые протоколы HTTP/HTTPS.

Лучшей практикой будет использование облачного решения. Однако облако, которое действительно защищает от DDoS-атак, должно обладать следующими свойствами:

- Распределенность. В облаке должно быть несколько географически разнесенных узлов, чтобы вывод из строя любого из них не оказывал влияния на сервис.
- Собственная автономная система и собственные адресные блоки, из которых для защищаемого сервиса выделяется новый IP-адрес, скрывающий истинное его расположение в сети.
- Глобальная связность автономной системы с Интернетом. Только магистральные операторы в качестве провайдеров облачных сервисов дадут уверенность клиентам, находящимся под защитой облачного решения, в том, что их трафик не будет теряться вне зависимости от того, какие атаки осуществляются.
- Полная автоматизация процесса фильтрации. У хорошей системы защиты от DDoS-атак – тысячи клиентов и сотни инцидентов в день. Этот объем невозможно обработать вручную. Ручное вмешательство порождает ошибки, так как человек должен оперативно решать, какие фильтры подключать и пр., что не всегда приводит к нужному результату.
- Постоянная фильтрация должна быть приоритетной услугой, поскольку любое переключение по протоколу BGP или DNS означает время простоя сайта, измеряемое десятками минут, и раскрытие истинного местоположения сервера.
- Использование технологии MPLS (multiprotocol label switching) VPN в качестве резервной связности системы защиты и сервера. Это позволит даже при полностью забитых "мусором" каналах дата-центра сохранить полную работоспособность сервера.
- SLA обязан включать в себя также и время атаки.

Приведем пример

Если фильтрация осуществляется в ручном режиме переводом DNS с TTL 5 минут (TTL – время жизни пакета данных в протоколе IP – предельно допустимое время его пребывания в системе), то сценарий может быть таким:

1. Начинается атака.
2. Дежурный по регламенту регистрирует ее факт (+5 минут).
3. Дежурный по регламенту звонит администратору сайта и обсуждает с ним, какие фильтры будут включены, чтобы, с одной стороны, защититься, с другой – чтобы не заблокировать легитимных пользователей. Без этого пункта нейтрализацию атаки можно было бы автоматизировать (+10–15 минут).
4. Перевод трафика, что составляет не менее TTL*2 (+10 минут).
5. Мониторинг и коррекция работы фильтров (+10–15 минут).

Итого, если все участники сработали штатно и по регламенту, реагировали достаточно быстро, то сервер заработает через 45 минут после начала атаки. Некоторые атакующие пользуются этим сценарием: они то снимают атаку, то возобновляют ее, получая недоступность защищаемого ресурса.

Сам сервер должен обладать рядом качеств, которые позволят ему быть всегда доступным для клиента:

- Возможность выдерживать рост легитимной нагрузки, чтобы не "падать" во время рекламных кампаний и быстро восстанавливаться, когда фильтры включились. Также важно понимать, что некоторое количество ботов (обычно 1–2%) может быть пропущено, и сервер должен быть способен это выдерживать.

"Один сервер – один сервис". Web-сервер должен быть на своем сервере единственным приложением. Иначе атакующая сторона узнает его IP, например из записи MX (Mail Exchanger – один из типов записей в DNS, указывающий способ маршрутизации электронной почты), или Web-сервер может быть выведен из строя исчерпанием ресурсов процессора за счет другого сервиса.

- Устойчивый распределенный DNS.

Какой бы метод защиты от DDoS ни выбрала компания, главное – помнить, что к атакам нужно быть готовым заранее. Кроме того, построенная IT-инфраструктура должна полностью соответствовать объемам бизнеса компании. Это поможет минимизировать ущерб и не потерять лояльность клиентов даже в самый активный бизнес-сезон. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Отметим

В последнее время атаки часто привязывают к "горячему" времени сезона продаж или к маркетинговой кампании. Это могут быть новогодние праздники, 8 марта, 23 февраля, когда некоторые отрасли коммерции получают самую большую выручку, а простой во время активной рекламы приведет к трате бюджета впустую и репутационным рискам.

Таблица 1. Статистика по числу уязвимых серверов, которые могут выступать в качестве амплификаторов, во всем мире

Chargen Amplification	70319
DNS Amplification	7064242
NTP Amplification	307744
SNMP Amplification	4411780
SSDP Amplification	18108954

Таблица 2. Статистика по числу уязвимых серверов, которые могут выступать в качестве амплификаторов, в России

Chargen Amplification	4616
DNS Amplification	299512
NTP Amplification	6931
SNMP Amplification	77635
SSDP Amplification	803077

Бизнес и ИБ: сотрудничество или противостояние?

Одной из главных проблем сегодня является взаимодействие сотрудников информационной безопасности и топ-менеджеров бизнеса. Для успешного развития ИБ должна защищать бизнес, но на деле получается, что бизнес не видит или не придает особого значения тем задачам, которыми занимается информационная безопасность, а сотрудникам службы ИБ не хватает знаний о бизнес-процессах, которые они защищают. Редакция журнала "Информационная безопасность/Information Security" спросила экспертов отрасли:

1. Как оценить реальные риски для бизнеса, которые несут киберугрозы?
2. Как доказать бизнесу необходимость защищаться от киберугроз?
3. Кто и как отвечает/должен отвечать за кибербезопасность предприятия?
4. Производители средств безопасности помогают решить бизнес-задачи предприятия или берут на испуг?
5. Требования регуляторов – необходимость или ярмо для бизнеса?

Роман Кобцев,
директор департамента развития и маркетинга компании "ЭЛВИС ПЛЮС"

1. ИБ, с одной стороны, давно стала неотъемлемой частью деятельности любого предприятия, а с другой стороны, по-прежнему страдает от остаточного принципа внимания к ней со стороны руководства бизнеса. Однако если даже бизнес-процесс напрямую не генерирует денежные потоки, это не значит, что он не способствует росту бизнеса.

Пару лет назад компания Ernst & Young провела исследование, как компании-лидеры управляют рисками в целях повышения эффективности деятельности. Выяснилось, что компании-лидеры рассматривают конкурентоспособность как способность предприятия в заданных условиях добиться бизнес-показателей выше, чем у конкурентов. И были выделены три основных группы факторов, помогающих организации улучшить бизнес-показатели:

1. Снижение уровня риска.
2. Создание добавленной стоимости.
3. Сокращение затрат.

Таким образом, можно сделать смелое предположение, что через снижение уровня риска ИБ способствует росту бизнеса предприятия.

2. ИБ-специалистам нужно всегда помнить: что бы мы там о себе ни думали, бизнес всегда будет обращать первостепенное внимание исключительно только на бизнес-риски. Поэтому сложно доказать бизнесу, что риски реализации киберугроз так же важны, как риски доступа к кредитам или риски медленного восстановления экономики. Исследования той же Ernst & Young в сфере бизнес-рисков показывают, что риски, связанные с реализацией угроз безопасности информации, или IT-риски редко попадают в ТОП-10 бизнес-рисков (из нескольких десятков отраслей только в трех такие риски попали в ТОП-10). Если я не ошибаюсь, это были телеком, банки и разработка новых технологий. Вот в этих отраслях, я думаю, и нет особых проблем с убеждением бизнеса в необходимости снижения IT-рисков и принятия мер кибербезопасности. Во всех остальных отраслях безопасникам чаще всего придется доказывать связь киберугроз с ущербом бизнесу. И такие меры, как демонстрация наличия уязвимостей и вероятности возможных атак, могут повлиять только на уровень управленцев той же IT или ИБ, а доказать топ-менеджеру, почему 10 лет у него ущерба от киберугроз не было, а сейчас вдруг произойдет, будет непросто. В любом случае, нужно попытаться максимально показать влияние современных вызовов ИБ на бизнес-риски организации, если есть карта рисков предприятия, или усредненно, на примере ТОП-10 бизнес-рисков отрасли, если управление рисками не формализовано. И не нужно бояться того, что не всегда можно применить количественные методики.

Если оценка качественная, это еще не значит, что она не дает объективной картины. К примеру, если мы видим дождь, выходя из дома, мы не рассчитываем количество воды, которая может проникнуть к нашему телу, процент снижения его температуры и сумму убытков в рублях от возможной неработоспособности, а также коэффициент вероятности всего этого – мы просто берем зонт. И незнание точных показателей совершенно не мешает нам жить в данной ситуации.

3. Такие вопросы, конечно, нужно детализировать: что имеется в виду? В любом случае за все риски несет ответственность генеральный директор. А дальше можно долго рассуждать, кто должен отвечать – IT-директор или служба безопасности, – или должно быть создано специализированное подразделение. Все зависит от масштабов предприятия и особенностей его рода деятельности.

4. Производители средств безопасности, конечно, заинтересованы в первую очередь в сбыте своих продуктов, но сказать, что они только берут на испуг, нельзя. Таким способом долго на рынке не продержишься. В enterprise-сегменте такие номера вообще чреваты, потому что покупатель, как правило, очень хорошо разбирается в вопросе, кроме того, может заказать экспертизу у конкурирующей организации для проверки на объективность. В потребительском сегменте, может, и можно продвигать свои продукты страшилками, но, на мой взгляд, B2C рынок у нас пока еще только на стадии созревания, и потребители не особо заморачиваются безопасностью (антивирус есть – и ладно). Конечно, в отношениях производителей и потребителей в нашей отрасли, может, и не всегда все гладко, но пока все-таки отношения лежат в плоскости общения равных профессионалов по сути вопроса, а не "выстраивания позитивных отношений с брендом" и др. маркетинговым фоном из жизни потребительских рынков.

5. Требования регуляторов в этой сфере были, есть и будут всегда, и наш рынок не самый зарегулированный, это мировые практики. Кроме того тенденции последних лет – это стремление государственных структур (преимущественно силовых) к усилению регулирования частного сектора в сфере ИБ. И это и в США, и в Европе. Другое дело, как это делать… ●

Павел Головлев,
начальник управления безопасности информационных технологий ОАО "СМП Банк"

1. Риск – это неотъемлемый атрибут бизнеса. Оценить его может только сам бизнес. На эту тему замечательно высказались создатели CyberSecurity Index Mukul Pareek и Daniel Earl Geer, Jr.: "Для того, чтобы быть действительно полезным, любой показатель безопасности должен удовлетворять, по крайней мере, двум требованиям:

I) Риск-менеджеры должны быть в состоянии использовать эту цифру для хеджирования рисков;

2) Инвесторы должны иметь возможность принять измеренный риск и получить большую прибыль по сравнению с теми, кто отказывается от этого риска".

2. Вопрос не совсем корректный. Доказать необходимость защищаться вообще от всего невозможно. Необходимо определить цели бизнеса, объекты защиты и актуальные угрозы. А также выбрать из возможных защитных мер те, которые снижают риск до приемлемого уровня с наименьшими затратами. Для этого необходимо уметь отвечать на вопрос: "Почему?" – и задавать вопрос: "Зачем?"

3. Вообще-то – все сотрудники, но каждый по-своему. Одним достаточно знать и выполнять элементарные правила "компьютерной гигиены", другие должны заниматься стратегическим планированием и ресурсным обеспечением, третьи – быть специалистами в предметной области и решать конкретные прикладные задачи. При этом роль первых ничуть не менее значима, чем остальных.

4. Необходимо понимать, что каждый производитель средств безопасности в первую очередь решает свою бизнес-задачу – получение прибыли. К сожалению, в отношениях с "бизнесом на ИБ" все чаще приходится перефразировать известный тост: "Так выпьем же за то, чтобы наши желания совпадали с их возможностями!"

5. Скажем политкорректнее: "дополнительная операционная нагрузка". Из-за того, что часто подобные требования принимаются на основании "социального заказа", они не всегда соотносятся с реальными рисками.

Так, расходы на реализацию последних изменений в Положении Центрального банка 382-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" в части усиления мер безопасности для банкоматов и терминалов легко могут превысить годовой ущерб от карточного мошенничества. Но ИБ в этом контексте – достаточно циничная "псевдонаука". То, что является существенным для одного человека или организации, совершенно теряется на фоне общей статистики. Несомненным является одно: сложившееся стремление к чрезмерному регулированию процесса вместо спроса за результат является помехой для бизнеса, каковы бы ни были его явные и скрытые причины. ●

Петр Ляпин,
начальник службы информационной безопасности "НИИ Транснефть"

1. Не буду оригинален. Сложно. И в большинстве случаев индивидуально. Существуют методики и критерии в форме международных и национальных стандартов, рекомендаций и лучших практик. Более частным случаем являются отраслевые методики (как стандарт Банка России). В любом случае, реальные риски бизнес должен оценивать самостоятельно. Бизнес сам ставит себе главную цель – извлечение прибыли. Декомпозирует ее, выстраивая свою функциональную модель, формирует все те процессы, которые и позволяют достичь главной цели. И риски влияния киберугроз должны рассматриваться именно в этом контексте.

2. Не нужно ничего доказывать. Обосновать предложенные меры – да, но не доказывать необходимость. Начинать всегда следует с начала. А начало это, в соответствии с ГК РФ, "самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли…". То есть решение, как жить и жить ли вообще, бизнес принимает всегда самостоятельно. Вот подготовить максимально полную и объективную информацию (по киберугрозам в частности) для принятия решения – это задача ИБ. В том числе информацию о предлагаемых мерах защиты от киберугроз (читай – снижения соответствующих рисков).

3. Важно понимать, что в соответствии с ГК РФ в первую очередь за кибербезопасность предприятия отвечает лицо, которое в силу закона или учредительного документа юридического лица уполномочено выступать от его имени. Дальше по отдельным направлениям ответственность распределяется между подразделениями и работниками предприятия в соответствии с ТК РФ, правилами внутреннего трудового распорядка, трудовыми договорами и должностными инструкциями. Эффективным видится деление ответственности на организационную и обеспечительную части. Первая относится к специалистам в области ИБ, вторая – ко всем работникам, задействованным в бизнес-процессах, которым присущи риски, связанные с кибербезопасностью. Иными словами, как выстраивать управление ИБ в целом, знает только специалист, а выполнять установленные правила ИБ обязан уже каждый работник, так же, как правила пожарной безопасности и охраны труда.

4. И то, и другое, разумеется, присутствует. Соотношение бывает различное, но здесь важно понимать простое исходное положение: производители средств безопасности – это в большинстве своем предприниматели, главной целью которых является извлечение прибыли. И способ извлечения этой прибыли определяется уже не столько безопасностью целевого предприятия и подобными категориями, а, скорее, законами рынка и технологиями продаж.

5. На этот вопрос однозначно не ответить, отчасти верно и то, и другое. Есть объективная действительность, которой просто опасно пренебрегать. Есть и "синтетика". Так, к первой категории можно отнести объективно сложившиеся требования, игнорировать которые ни одному участнику системы нельзя, так как это с высокой степенью вероятности скажется негативно не только на нем, но и на всей системе. Не важно, как субъект выполняет требования, нести ответственность за последствия их нарушения он будет при любых обстоятельствах. Ко второй категории в качестве яркого примера можно отнести такой образец законотворчества, как Федеральный закон "О персональных данных", особенно в его последней редакции. Для понимания вопроса не лишним здесь будет вернуться к исходным положениям Конвенции Совета Европы № 108, где речь, например, идет о защите частных лиц, а не ПДн. ●

Вопросы обработки ПДн третьих лиц на примере "контактных" лиц заемщика: уроки практики

Алексей Чирков, *советник по правовым вопросам, Российский микрофинансовый центр*

Настоящая статья посвящена вопросам обработки ПДн третьих лиц, в отношении которых у оператора отсутствует правовое основание обработки, но существует необходимость, диктуемая выстроенными бизнес-процессами. Рассматриваются возможные подходы к решению данной задачи с учетом практики.

В настоящее время многие операторы ПДн в ходе осуществления своей деятельности сталкиваются с необходимостью обработки персональных данных третьих лиц, с которыми у оператора отсутствуют какие-либо отношения и чьи данные получены без их согласия от третьих лиц. Строго говоря, в большинстве таких случаев ни одно из оснований, указанных в ст. 6 Федерального закона от 27.07.2006 ФЗ № 152 "О персональных данных" (далее – ФЗ № 152), не является применимым, однако практика заставляет рассматривать возможные способы их законной обработки. В качестве примера практической ситуации возникновения такой потребности рассмотрим следующий пример.

Заемщик-гражданин обращается в банк или иную финансовую организацию[1] с заявлением о предоставлении потребительского кредита. Наличие в таком заявлении телефонов и иных контактных данных родственников, друзей, родителей заемщика повышает (в случае возникновения просрочки) вероятность успешного взыскания долга, по разным оценкам, на 20–40%. Таким образом, в описанной ситуации возникает необходимость обработки ПДн так называемых "контактных" лиц (далее – ситуация), однако правомерность такой обработки неочевидна. Практика выработала, как минимум, три способа[2] юридического оформления обработки в приведенной ситуации, которые будут рассмотрены далее.

Суть проблемы

В описанном выше примере ПДн субъекта получаются без его согласия от третьего лица. При этом в соответствии с ч. 1 ст. 6 ФЗ № 152 перечень случаев, когда ПДн могут законно обрабатываться без согласия лица, которому они принадлежат, исчерпывающе определен. И описанная ситуация в этот перечень не попадает. Во-вторых, в соответствии со ст. 18 ФЗ № 152 в случае, когда ПДн получены не от субъекта, которому они принадлежат, оператор обязан уведомить субъекта о факте обработки его ПДн и сообщить ему определенный перечень информации, что создает еще одну сложность. К тому же вполне очевидно, что реализация такой обязанности оператором в ряде случаев может повлечь законное требование субъекта о прекращении обработки его ПДн. Это создает юридические сложности в описанной выше ситуации. На практике появилось как минимум три варианта соблюдения норм ФЗ № 152 при обработке ПДн "контактных" лиц – без их согласия и уведомления.

Данные не персональные

Смысл первого варианта состоит в том, чтобы доказать, что обрабатываемые данные не являются персональными. Это представляется возможным в следующих случаях. Во-первых, объем собираемой информации должен ограничиваться контактным номером телефона и именем. В случае, если о "контактном" лице запрашивается и степень родства заемщику, и паспортные данные, и другая дополнительная информация, такой вариант вряд ли применим. Во-вторых, требуется корректное оформление анкеты. Например, исходя из правоприменительной практики, строчка в анкете "предпочитаемое обра-

[1] *С 01.07.2014 предоставлять займы заемщикам-потребителям (то есть осуществлять профессиональную деятельность по предоставлению потребительских займов) могут исключительно следующие финансовые организации: кредитные (в том числе банки) и микрофинансовые организации, ломбарды, кредитные кооперативы.*

[2] *В настоящей статье не рассматривается вариант, при котором заемщик действует как представитель контактного лица на основании доверенности. Во-первых, такой вариант прямо вытекает из закона, во-вторых, он вряд ли возможен в большинстве типичных сделок профессионального кредитора, поскольку оригинал доверенности с подписью контактного лица большинство заемщиков представить не могут.*

Комментарий эксперта

Любовь Шорина,
консультант практики аудита и консалтинга компании "Астерос Информационная безопасность"

Обеспечение правомерности обработки ПДн, полученных не от субъекта персональных данных, действительно является одним из наиболее сложных моментов применения ФЗ № 152, поскольку в большинстве случаев требует наличия согласия и уведомления субъектов на обработку их персональных данных (ст. 6 и 18 ФЗ № 152 соответственно), а также обязательного подтверждения лицом, которое предоставляет оператору персональные данные субъекта, наличия у него правовых оснований для их обработки (ст. 9 ФЗ № 152).

Такое количество не вполне согласованных между собой требований зачастую вызывает массу вопросов и сложностей в попытке спроецировать их на конкретную ситуацию. Причем проблемы возникают даже в том случае, когда персональные данные предоставляются юридическим лицом, например кадровым агентством. Однако если в заключенном между компаниями договоре можно прописать соответствующие обязанности сторон в части соблюдения требований ФЗ № 152, то ситуация несколько упрощается.

Рассмотренные автором статьи варианты соблюдения требований ФЗ № 152 на практике при обработке персональных данных "контактных" лиц представляют несомненный интерес и еще раз подчеркивают несовершенство данного закона, так как для его выполнения операторам приходится изобретать столь изощренные и неоднозначные схемы. С практической точки зрения наиболее удобен последний из рассмотренных вариантов. При этом необходимо уточнить, что для корректного оформления поручения обработки персональных данных "контактных" лиц до предоставления заполненной анкеты финансовой организации заемщик должен заключить с ней договор, прописав в нем условия поручения и обязанности финансовой организации в соответствии с ч. 3 ст. 6 ФЗ № 152.

И в завершение хочется отметить, что тщательный анализ процессов обработки и исключение сбора избыточных ПДн позволит в дальнейшем избежать многих проблем. Тем более что данный принцип озвучен в самом ФЗ № 152. Так, например, в анкете кандидата на трудоустройство лучше запрашивать не ФИО, должность и контактные данные рекомендателя кандидата, а название и контактный телефон компании, в которой ранее работал специалист. ●

щение или псевдоним" с точки зрения отношения данных к персональным выглядит значительно лучше, нежели классическое "ФИО", поскольку предполагает возможность различного заполнения – от имени до социального статуса. В этом случае вероятность признания имени ПДн крайне низка. В-третьих, необходимо подготовить соответствующую аргументацию по вопросу неотнесения к ПДн номера телефона контактного лица. В теории номер телефон может быть классифицирован как обезличенные персональные данные, так как установить принадлежность совокупности цифр конкретному лицу возможно только при доступе к базе оператора связи. Юридически для финансовых организаций это невозможно. В судебной практике в подобных ситуациях номер телефона, как правило, не признается ПДн, поскольку расценивается не относящимся к конкретному лицу[3]. Таким образом, одним из вариантов обработки информации о "контактных" лицах должника является сбор данных в объеме, достаточном для взаимодействия с контактным лицом, но недостаточным для признания их персональными.

Данные заемщика, а не контактного лица

Этот вариант может быть реализован путем запроса у заемщика, к примеру, большего числа номеров, чем имеет "обычный" заемщик. К примеру, вместо привычных граф анкеты-заявления о предоставлении потребительского кредита (займа) (далее – заявление) "домашний" и "мобильный телефон" можно использовать четыре или пять обязательных для заполнения граф "номер телефона". Вероятно, 2 или 3 номера в таком заявлении будут принадлежать не самому заемщику, а третьим лицам. Однако юридически при наличии в заявлении фразы вроде "достоверность указанных сведений, а также их принадлежность лично мне подтверждаю" финансовая организация вправе законно обрабатывать все указанные данные, в том числе и номера телефонов. Помимо согласия в самом заявлении это право базируется и на принципе добросовестности, закрепленном в ГК РФ: финансовая организация вправе добросовестно полагаться на достоверность сообщаемых заемщиком сведений.

Финансовая организация как обработчик

В данном случае в подписываемом заявлении содержится поручение заемщика, который в роли оператора[4] поручает финансовой организации обрабатывать ПДн субъекта (контактного лица) "в целях доведения информации о просроченной задолженности оператора до субъекта персональных данных" определенными в заявлении способами. Данная схема при корректном юридическом оформлении имеет ряд преимуществ перед двумя предыдущими: о контактном (или любом третьем лице) могут быть сообщены любые ПДн; финансовая организация, выступая применительно к ПДн контактного лица "лицом, осуществляющим обработку персональных данных по поручению оператора", не несет никакой ответственности перед самим контактным лицом, которое может обращаться с жалобами в уполномоченный орган. Ответственность за нарушения при обработке ПДн у финансовой организации в этом случае есть только перед заемщиком-оператором ПДн контактного лица. Перед самим же "кон-

[3] *См., например, Апелляционное определение Московского городского суда от 28.01.2014 по делу № 33-5461.*

[4] *Оператором, в соответствии с ФЗ № 152, признается государственный муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и/или осуществляющие обработку ПДн, а также определяющие цели их обработки, состав и действия (операции), совершаемые с ними. Таким образом, юридических препятствий, вопреки мнению отдельных экспертов, для признания физического лица оператором ПДн не существует.*

тактным" лицом за все нарушения, в том числе возможно допущенные финансовой организацией, будет отвечать заемщик.

Получая таким образом ПДн, финансовая организации освобождается от обязанности предоставления информации, предусмотренной ч. 3 ст. 18 ФЗ № 152 для ситуаций, когда информация получена не от самого субъекта.

Таким образом, данная схема позволяет обрабатывать ПДн третьего лица, не получая непосредственно от него согласия.

Итог

Это основные встречающиеся на практике решения по обработке ПДн "контактных" лиц. Возможно, не все из них полностью соответствуют духу законодательства о защите персональных данных, однако ни одно из них, по имеющимся данным, не повлекло привлечения к ответственности, равно как и не вызывало вопросов прокуратуры и Роскомнадзора при проведении проверок в финансовых организациях.

Однако вне зависимости от того, каким образом были получены данные заемщика, представляется крайне важным проверять их достоверность, причем проверять в момент получения, а не тогда, когда возникает необходимость их использования. Несоблюдение именно этого требования часто становится причиной обращений субъектов ПДн к операторам и уполномоченному органу.

В случае, если указанные данные не принадлежат заемщику, то для их удаления финансовая организация вправе потребовать личного визита третьего лица, которому принадлежат эти данные, в свой офис для предоставления документов, подтверждающих принадлежность указанных телефонов этому третьему лицу (например, абонентского договора), а не указавшему их заемщику. Данная позиция в настоящее время поддерживается как минимум двумя территориальными управлениями Роскомнадзора. Данный способ (его весьма сложно назвать некой схемой адаптации к требования законодательства) достаточно активно используется на практике; ответственность в такой ситуации может понести лишь сам заемщик, указывающий чужие ПДн.

Очевидно, ничто изложенное в настоящей статье не означает одобрения или тем более прямой рекомендации по использованию описанных схем. Однако, как представляется, в определенных случаях подобный анализ практики может быть полезен при выработке собственных юридических решений подобных ситуаций. Решений, основанных на букве закона и соответствующих его духу. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Тесты антивирусов

Часть 2

Дмитрий Беликов, *студент 6 курса МИЭМ НИУ ВШЭ*
Александр Сорокин, *старший преподаватель кафедры компьютерной безопасности МИЭМ НИУ ВШЭ*
Ксения Чурсина, *студентка 6 курса МИЭМ НИУ ВШЭ*

Разобравшись в предыдущей статье с тем, какие тесты важны для оценки качества антивирусов, постараемся теперь решить вопрос поиска авторитетных источников результатов рассмотренных тестов.

Кто тестирует?

Сравнения антивирусных средств стали проводиться достаточно давно, и в конце концов накопилось значительное количество методик, наработок, идей, которые требовали какой-то структуризации.

В 2008 г. в Бильбао (Испания) была основана международная некоммерческая организация AMTSO1 (Anti Malware Testing Standards Organization – Организация по стандартизации тестирования средств защиты от вредоносных программ). Своей целью она поставила выработку и совершенствование корректных, объективных тестовых методик. Членами организации являются разработчики, тестировщики, ученые (как компании, так и частные лица).

В состав данной организации входит достаточно большое число как независимых тестовых лабораторий (AV-Comparatives, AV-Test, Virus Bulletin, PC Security Labs и др.), так и производителей антивирусного ПО, среди которых много известных поставщиков (AVG, Agnitum, Avira, ESET, Avast, IBM, Kaspersky Lab, Panda Security, Trend Micro, Symantec, Sophos, Bitdefender и др.).

Следует отметить, что данная организация не занимается проведением тестов, а ее деятельность направлена исключительно на выработку стандартов и рекомендаций для тех, кто занимается тестированием. Так как в состав AMTSO входит значительное количество различных производителей, эти рекомендации достаточно объективны и не дают преимуществ какому-либо конкретному поставщику.

Далее приведем обзор тестовых лабораторий, которые входят в состав AMTSO или пользуются популярностью у пользователей антивирусного ПО.

Лаборатории

AV-Comparatives[2]

Австрийская лаборатория. Проводит большое количество различных тестов (почти все из рассмотренных в прошлой статье) с рейтингованием по каждому из них. По результатам каждого теста публикуется большой отчет (раз в несколько месяцев), содержащий описание тестируемых продуктов, методику, результаты.

Плюсы: публикуются подробные отчеты, наиболее полный набор различных тестов.

Минусы: не во всех тестах на протяжении года участвуют один и тот же набор (речь идет как о версиях продуктов – Free/Pro/Internet Security, – так и о поставщиках).

AV-Test[3]

Немецкая лаборатория. Проводит тесты в трех категориях (защита, производительность, удобство использования), результат представляется большой сводной таблицей (отдельно по каждой из операционных систем).

Плюсы: большое количество тестируемых антивирусов, каждый из них тестируется отдельно для каждой операционной системы (Home User: Win XP, Win Vista, Win 7, Win 8; Corporate User: Win XP, Win 7, Win 8; Android), интегрированная оценка.

Минусы: мало конкретики, не приводятся отчеты о самих тестах, на основе которых были получены оценки.

Dennis Technology Labs[4]

Небольшая английская тестовая лаборатория, родоначальники AMTSO, специализируется на "жизненных" тестах.

Плюсы: подробные отчеты с описанием методики тестирования.

Минусы: небольшое число тестируемых антивирусных средств.

Virus Bulletin[5]

Английский ресурс, один из старейших по антивирусной тематике (выходил в виде журнала с 1989 г.). Проводит тестирования только по "классической" модели. На основе тестирования формируется таблица с результатами в формате "прошел/не прошел" в различных категориях (метка "прошел" означает получение сертификата VB). Подробные отчеты представляются только по запросу и являются платными.

Плюсы: сертификат получают только антивирусы с соотношением 100 обнаруженных/0 ложных срабатываний.

[1] *Со всеми документами можно ознакомиться в разделе "Документы" (Documents) на официальном сайте организации: http://www.amtso.org/documents.html*
[2] *http://www.av-comparatives.org/*
[3] *http://www.av-test.org/*
[4] *http://www.dennistechnologylabs.com/*
[5] *https://www.virusbtn.com*

Минусы: платность полных отчетов; не учитывается производительность и качество лечения; сертификаты даются по каждому из отдельных тестов, включая легкие, поэтому факт наличия сертификата не гарантирует высокого качества антивируса, для более объективной оценки требуется проверка на сайте VB по всем категориям.

AV-Lab[6]

Польская тестовая лаборатория. Делает упор на тестирование "в реальном времени". Оно представляет собой тест в условиях использования, приближенных к реальным, когда антивирусу не "подсовывают" за раз тысячи инфицированных файлов, а заставляют его периодически сталкиваться с угрозами. Используется 40 образцов в день для одной антивирусной программы (20 для динамического тестирования и 20 на проверку вредоносных Web-ссылок), чтобы ситуация была наиболее приближена к реальной работе пользователя в тестируемой системе.

Плюсы: постоянно обновляемая информация с итоговыми отчетами за отчетный период, интуитивная понятность визуализированных результатов.

Минусы: польский язык и ориентация на польского потребителя в целом.

ICSA Labs[7]

Независимое подразделение Cybertrust, Inc, занимается исследованиями, испытаниями и сертифицированием продуктов безопасности, включая антивирусы, межсетевые экраны, средства криптографии, антишпионские программы и т.д. Результат исследований лаборатории – выдача или не выдача сертификата.

Плюсы: ежемесячные отчеты, опыт организации в тестировании не только антивирусных ядер, но и других средств безопасности (которые сейчас в подавляющем большинстве случаев входят в состав антивирусного ПО).

Минусы: отсутствие подробных отчетов (результаты предоставляются в виде таблицы с результатами вида "прошел/не прошел").

Comparative Testing Labs	Real-World Protection Test	Number of test cases per month	File Detection Test	Number of test cases	Behavioral Test	Performance Test	Malware Removal Test	Included products
AV-Comparatives	✓	~500 (~2000 per report)	✓	~150000	✓	✓	✓	~25
AV-Test	✓	~50 (~100 per report)	✓	~20000	✗	✓	✗	~25
Dennis Technology Labs	✓	~30 (100 per report)	✗	N/A	✗	✗	✗	~10
PC Security Labs	✓	N/A	✓	~20000	✓	✓	✗	~25
VirusBulletin	✗	N/A	✓	~3000	✗	✗	✗	~50

Рис. 1. Сводная таблица, характеризующая несколько наиболее популярных тестовых лабораторий. Подготовлена AV-Comparatives*

West Coast Labs[8]

В целом аналогичная американская сертификационная лаборатория.

PC Security Labs[9]

Китайская лаборатория. Периодически проводящая, помимо "классического" статического теста, различные тесты со специфической направленностью (тесты по ресурсоемкости и мобильной безопасности).

Плюсы: большое число тестируемых продуктов, достаточно редкие тесты (Android – редко встречается у крупных лабораторий, а не у индивидуальных обозревателей), подробные отчеты с методикой тестирования (тесты на ресурсоемкость состоят из 12 отдельных тестовых исследований).

Минусы: небольшое разнообразие тестов для компьютерных антивирусов (например, отсутствует динамическое тестирование).

Anti-Malware Test Labs[10]

Российский ресурс. Проводит собственные тесты, а также публикует последние новости в области программных средств компьютерной безопасности.

Плюсы: подробные отчеты, содержащие методику тестирования, сравнение не только классических антивирусов, но и межсетевых экранов, систем предотвращения вторжений.

Минусы: отсутствие какого-либо плана тестов. Тесты делаются независимо друг от друга в различное время, часто с большими перерывами и с совершенно различным набором продуктов.

TopTenReviews[11]

Проводит большое количество сравнений различного ПО (антивирусы, средства для работы с CD/DVD, фотообработки), мобильных устройств, электроники и т.д.

Плюсы: разнообразие проводимых тестов, наглядная визуализация результата.

Минусы: отсутствие подробных отчетов, большое количество рекламы на странице с результатами.

Другие лаборатории

- MRG Effitas (http://www.mrg-effitas.com/) – английская лаборатория, специализируется на интернет-безопасности (браузеры, онлайн-банкинг).
- NSS Labs (https://www.nss-labs.com/) – американская лаборатория, изучающая антивирусы, межсетевые экраны, системы обнаружения атак, социальную инженерию на коммерческой основе, более известна благодаря тестированиям аппаратного обеспечения.
- Tolly Group (http://www.tolly.com/) – американская лаборатория, специализирующаяся на тестах и сертификации крупных вендоров.
- Matousec (http://www.matousec.com/) – чешский проект, созданный для тестирования межсетевых экранов, проводит тесты проактивной защиты антивирусов.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

* Данная таблица составлена лабораторией AV-Comparatives и поэтому не описывает всю картину в целом, так как скрывает некоторые недостатки AV-Comparatives и плюсы других лабораторий.

Но даже в таких условиях таблица достаточно наглядно показывает, что идеальной лаборатории, которая тестировала бы все продукты, проводя при этом все возможные типы тестов, не существует. Выбирая антивирусное средство, следует руководствоваться результатами тестирования различных лабораторий. А для выбора наиболее надежных – можно ориентироваться на рейтинг доверия пользователей и на авторитет среди производителей антивирусного ПО.

[6] http://avlab.pl/
[7] https://www.icsalabs.com/
[8] http://www.westcoastlabs.com/
[9] http://www.pcsecuritylabs.net/
[10] http://www.anti-malware.ru/
[11] http://www.toptenreviews.com/

Защититься реально – труднее доказать, что это нужно

Леонид Яшин, *заместитель начальника Департамента платежных технологий Пробизнесбанка (ФГ Лайф)*

На сегодняшний день у каждого трудоспособного россиянина имеется банковская карта, с помощью которой он совершает платежи и проводит различные операции. Однако далеко не каждый держатель задумывается над тем, насколько защищена его карта, может ли он быть уверен в том, что хранящиеся на ней средства не исчезнут безвозвратно.

Области использования банковских карт: основные тенденции

В каких сферах использовали банковские карты клиенты Финансовой Группы Лайф в 2013–2014 гг.? Статистика (рис. 1) говорит о том, что в прошлом году клиенты активно использовали карты для снятия наличных и проведения различных операций в банкоматах, для оплаты товаров на предприятиях торговли и в Интернете. Однако в этом году объем денежных средств, снятых в банкомате, немного снизился. Зато повысился объем операций, связанных с выдачей наличных в кассах банка. Это свидетельствует о том, что клиенты банков перестали доверять банкоматам, на которые мошенники могут установить скимминговые устройства. Поэтому они предпочитают снимать деньги в кассе, где, на их взгляд, наиболее безопасно осуществлять подобные операции.

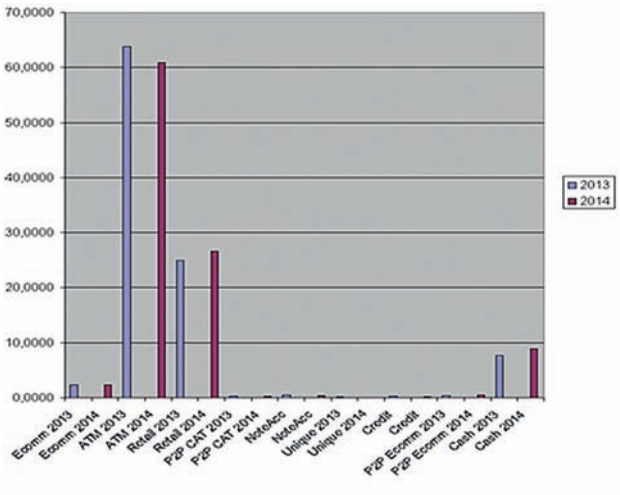


Рис. 1. Сферы использования пластиковых карт

По сравнению с прошлым годом увеличилось число операций, связанных с переводом денежных средств с карты на карту (P2P). Данный сервис был внедрен платежными системами сравнительно недавно. В банкоматах проведение таких переводов защищено (необходимо вводить PIN-код). Однако в Интернете эта функция не обладает надежной степенью защиты, так как в Интернете нередко требуется ввести номер карты и ее срок действия. Если карта не подключена к системе 3D-Secure, она не пройдет вторую аутентификацию, и мошенник, зная номер карты и срок действия (этих данных вполне достаточно), самостоятельно проведет операцию перевода. В наибольшей степени мошенническим атакам подвержены неперсонализированные переводы, для совершения которых не нужно вводить персональные данные (регистрироваться в банке, вводить ФИО). Такие переводы можно сравнить с переводами через телеком-провайдеров.

Нужен ли современному банку свой или аутсорсинговый фрод-мониторинг?

Нет сомнений в том, что у каждого участника платежных операций должен быть свой мониторинг мошеннических операций. Его отсутствие не освобождает от ответственности. За отсутствие мониторинга банк может быть оштрафован или вовсе лишен лицензии. Остается только определить, какой мониторинг нужен современному банку – свой или аутсорсинговый?

Ответ на данный вопрос зависит от схемы размещения процессинга банка. На банк-эквайер при соблюдении некоторых условий надеяться можно. Что касается своего банка, то здесь есть одна важная особенность: если банк соединен с банком-спонсором по межхостовому соединению, то в данном случае желательно иметь собственный мониторинг, поскольку существуют мошеннические операции, которые банк-спонсор может не заметить. Однако если свой процессинг находится в системе банка-спонсора, то имеет смысл воспользоваться его фрод-мониторингом, так как он видит операции не только в вашем банке, но и в других банках-спонсорах, и у него больше возможностей для анализа и противодействия мошенничеству. Что касается платежных систем, у них также имеется свой фрод-мониторинг, с помощью которого они видят множество подключенных к ним банков.

Какой мониторинг нужен современному банку – свой или аутсорсинговый? Ответ на данный вопрос зависит от схемы размещения процессинга банка.

В любом случае перед тем как выбрать, к какому банку подключаться, необходимо проанализировать ситуацию на рынке и возможности, которыми обладают банки, предоставляющие подобные сервисы.

Основные методы защиты и сервисы платежных систем

На сегодняшний день существует довольно много методов, которые защищают банковские карты. Однако все они обеспечивают защиту в проведении

AMT GROUP

ИСКУССТВО ИНТЕГРАЦИИ

ЗАЩИТА АСУ ТП

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНОГО ДОСТУПА

ЗАЩИТА ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

СЕРТИФИКАЦИОННОЕ ПРОИЗВОДСТВО

ЗАЩИТА ИНФРАСТРУКТУРЫ

+7 (495) 725-7660

www.amt.ru

БИЗНЕС - ЭТО ЛЮДИ

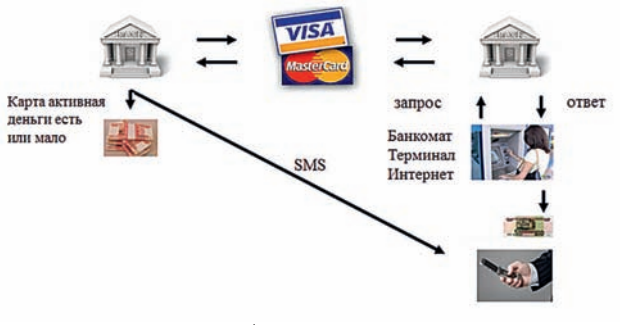


Рис. 2. Текущая схема прохождения платежей

3-D Secure является XML-протоколом, который используется как дополнительный уровень безопасности для онлайн-кредитных и дебетовых карт, двухфакторной аутентификации пользователя.

операций лишь в какой-то определенной области. На текущий момент не существует ни одного элемента защиты, который в совокупности защищал бы и в банкоматах, и в ритейле, и в Интернете.

Карточные методы защиты

Некоторое время назад одним из карточных методов защиты являлась подпись держателя карты, которая располагалась на задней панели карты и могла спасти при проверке карты в розничном магазине при случае, если мошенник решил воспользоваться именно ей. Однако подпись спасает далеко не от любых подделок: мошенникам достаточно сделать копию карты, расписаться на ней и осуществлять платежи от лица держателя карты.

Биометрия, несомненно, является следующим шагом в развитии идентификации клиентов, ее нужно развивать и улучшать.

Реальным способом защиты на всех этапах должна стать двойная аутентификация, которая может снизить вероятность кражи средств до 0%.

Следующий элемент защиты – код CVV1, располагающийся на магнитной полосе. Однако мошенники могут скопировать магнитную полосу и несанкционированно воспользоваться картой.

Самым распространенным элементом защиты является PIN-код. Он может спасти при операциях, в которых запрашивается ввод PIN-кода, но не может защитить от несанкционированного списания средств в Интернете и в розничном магазине без PIN-кода.

CVV2 позволяет защищать платежи в Интернете, но используется он не всегда и также не защищает от несанкционированных действий в розничном магазине.

Одним из надежных средств защиты считается система 3D-Secure, которая защищает оплату с карты в Интернете в 3D-магазинах. Если карта подключена к этой системе, то при оплате она пройдет двойную аутентификацию, что позволит надежно защитить хранящиеся на ней средства при условии, что клиент подключил услугу в банке.

Такие элементы защиты, как чип, PayPass и payWave, защищают карту от подделки в чиповых устройствах, но не защищают от несанкционированного списания в Интернете, в нечиповых устройствах и при краже.

Банковские элементы защиты

Среди банковских элементов защиты следует назвать установление лимитов сумм и их количества по операциям выдачи наличных в торговых предприятиях; ограничение типов операций в зависимости от продукта карты; ограничение операций в рискованных MCC (крупные аптеки, покерный бизнес и др.).

Кроме этого, банки проводят онлайн- и офлайн-мониторинг операций, приводящий либо к блокировке карты, либо к ограничению ее использования. Не менее важными являются рекомендации платежных систем, а также активное использование их сервисов (MATCH, MOST, MRP, SAFE, ADPS, CAMC).

Одним из новейших методов защиты является технология идентификации держателя карты. Биометрия, несомненно, является следующим шагом в развитии идентификации клиентов, ее нужно развивать и улучшать.

За мошенничество платежные системы перекладывают ответственность либо на эмитента, либо на эквайера, а процесс опротестования выходит очень затратным и занимает довольно длительное время. В проигравших остается либо банк, либо клиент, но не мошенник – он свое уже унес.

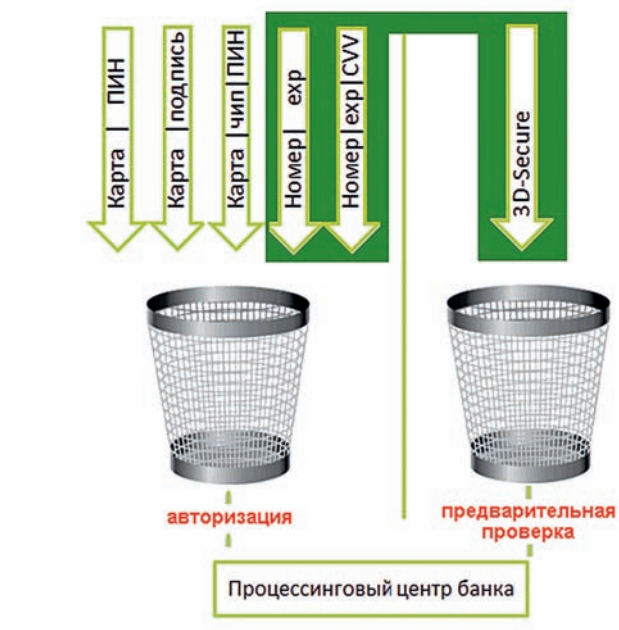


Рис. 3. Текущая защита транзакций

Важный элемент защиты платежей – двойная аутентификация

Текущая схема прохождения платежей выглядит, как показано на рис. 2.

Во время прохождения платежей чип, PIN-код, CVV и номер карты находятся в одном месте в один и тот же момент, что позволяет злоумышленникам компрометировать карты, поскольку нет элемента защиты, который защищал бы карту на всех этапах. Это можно сравнить с открытой дверью, а номер карты с адресом, куда должен прийти мошенник и забрать деньги.

Реальным способом защиты на всех этапах должна стать двойная аутентификация, которая может снизить вероятность кражи средств до 0%. На текущий момент при использовании технологии 3D-Secure в Интернете карта вначале проверяется одной системой защиты, которая дает разрешение на проведение операции, после чего поступает запрос на введение номера карты и ее срока действия (рис. 3).

Рис. 4. Ожидаемая защита транзакций

Следует отметить, что карта у пользователя, как правило, не заблокирована, а это значит, что злоумышленник может воспользоваться ее данными в любой момент.

Что же может помочь защитить карту при проведении операций и блокировать карту при ее неиспользовании?

Смысл технологии двойной аутентификации заключается в следующем. Изначально карта находится в блоке (неактивирована). Разблокировать ее перед операцией необходимо с помощью СМС путем введения определенных кодов. После этого можно воспользоваться картой в Интернете или банкомате, затем карта вновь будет заблокирована. Даже если на одном из этапов проведения операций мошенники скопируют данные карты, они не смогут ими воспользоваться, так как карта будет заблокирована, а код, пришедший по СМС для разблокировки, будет им неизвестен. Если им все же удастся скомпрометировать второй канал операции (СМС), то данные, содержащиеся в сообщении, не будут отражать информацию о том, к какой карте они относятся (рис. 4).

Двусторонний метод аутентификации позволяет защитить карту везде: и в банкомате, и в ритейле, и в Интернете. Затраты на его внедрение минимальны, поскольку не требуется сертификации от платежных и других систем, а банк может внедрить данную технологию самостоятельно. Антифрод-система банка сможет показать все неуспешные попытки по карте и выявить компрометацию без потери средств. А клиент сможет продолжать пользоваться картой даже при компрометации одного из каналов.

Таким образом, двойная аутентификация – очень важный метод защиты пластиковых карт. Банк, который начнет развивать данную технологию, будет иметь конкурентное преимущество на рынке по противодействию мошенничеству. ●

Двойная аутентификация – очень важный метод защиты пластиковых карт. Банк, который начнет развивать данную технологию, будет иметь конкурентное преимущество на рынке по противодействию мошенничеству.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

"МультиКарта": ресертификация на соответствие PCI DSS 3.0

ООО "МультиКарта" и компания "Инфосистемы Джет" сообщают об успешной ресертификации процессинговой компании на соответствие требованиям новой версии международного стандарта по защите информации в индустрии платежных карт PCI DSS 3.0.

Проект ресертификации затронул все основные системы и процессы, обеспечивающие безопасность хранения, обработки и передачи данных платежных карт. В ходе его реализации были учтены не только новые, более строгие требования стандарта PCI DSS, но и актуальные потребности "МультиКарты", связанные с необходимостью обеспечения непрерывности бизнеса и с завершением работ по объединению с "ТрансКредитКард".

Основным партнером проекта стала компания "Инфосистемы Джет", обладающая статусами Qualified Security Assessor (QSA) и Approved Scanning Vendor (ASV). Эксперты компании провели комплексное обследование архитектуры и взаимодействия всех системных компонентов, входящих в состав сложной IT-инфраструктуры "МультиКарты". Она включает более 60 серверов, расположенных на двух площадках – в Москве и Санкт-Петербурге. Следующим шагом стали работы по совершенствованию и оптимизации существующих процессов в соответствии с новыми требованиями стандарта PCI DSS, которые осуществлялись с участием специалистов компании "МультиКарта".

На завершающем этапе отдельная команда специалистов компании "Инфосистемы Джет" провела сертификационный аудит. Проводилась проверка систем, осуществляющих обработку и хранение данных платежных карт, регламентирующих документов и процедур, конфигураций используемых средств защиты. По результатам составлено заключение о полном соответствии процессинговых центров "МультиКарты" требованиям PCI DSS.

Результаты проведенного аудита приняты международными платежными системами Visa и MasterCard и подтверждены сертификатом о полном соответствии "МультиКарты" требованиям стандарта PCI DSS 3.0. ●

Мошенничество на АЗС

Игорь Решетников, *президент ООО "Нефтегазсофтсервис", руководитель российского MES-центра*

Не будем касаться громких дел и больших сфер, а поговорим о том, что может встретить каждый из нас.

Почти все мы – автолюбители, и, хочется этого или нет, надо время от времени заезжать на автозаправочные станции. Это самый близкий к нам сегмент топливно-энергетического комплекса. Казалось бы, все просто: на топливо-раздаточной колонке стоит счетчик, который должен проходить периодические проверки, касса автоматически выбивает чек. Все представляется совершенно прозрачным. Но, оказывается, АЗС являются просто клондайком для мошенников, причем страдают не только, потребители, но, часто даже в большей степени, владельцы сетей. Обычно – сами об этом не подозревая. Про разницу "покупаем в килограммах, продаем в литрах" знают все. Но вот что будет, если по сговору в емкости было залито топливо несертифицированного производителя? Сколько раз нам говорили, что сломался кассовый аппарат или что сначала выдается предварительный чек, а за фискальным надо подойти. Вы всегда за ним возвращаетесь? А все это и многое другое – источник проблем для нас и нелегального дохода для кого-то. Дополнительного контролера на каждой АЗС не поставишь, а если и поставишь, то где гарантия, что он не войдет в сговор с остальными? Поставить еще одного над всеми? А вопрос не такой уж и ничтожный: по имеющейся европейской статистике, в одной сети, в которой около 200 АЗС, в год регистрируется и пресекается подозрительных операций на сумму около миллиона евро. Не считая репутационных потерь, которые в условиях жесткой конкуренции не менее значимы.

В какой-то момент стало интересно: как же с этим борются? Выяснилось, что для мониторинга и анализа всего, что происходит на АЗС, успешно применяются системы класса Complex Event Processing (CEP), даже есть отдельный класс систем Fuel Fraud Detection (FFDS). Суть системы крайне проста: в режиме реального времени обрабатывается поток данных от всех точек возникновения информации на АЗС: объем горючего в резервуарах, документы на поставку топлива, расход топлива через ТРК, распечатка чека на ККМ и т.д.

При анализе соответствий между отдельными показателями по набору правил выявляются "странные", с точки зрения системы, события. Например, ни с того, ни с сего увеличился уровень горючего в резервуарах. Или расход горючего через ТРК не сопровождался распечаткой чека. Или объем залитого в резервуары топлива отличается от накладной, и т.д. и т.п. Даже с такой простой, с точки зрения реализации, системы можно получить уйму полезных данных и оперативно отслеживать все подозрительные операции на колонках, систематизировать и документировать необычные события, выдавать топ-менеджменту анализ ситуации и оперативно выявлять попытки мошенничества. По той же статистике для сети из 200 АЗС, для анализа фиксируется около 7 млн событий в день, что не так уж и много с точки зрения потока данных и легко обрабатывается и анализируется.

Очень хотелось бы, чтобы и в России владельцы сетей АЗС обратили внимание на борьбу с такими явлениями и перестали, наконец, просто включать эти потери в цену бензина. ●

Комментарий эксперта

Алексей Косихин, *руководитель направления по работе с ПиТЭК Центра информационной безопасности компании "Инфосистемы Джет"*

Краеугольный камень борьбы с фродом в ТЭК – комплексный подход

Тема мошенничества в данный момент актуальна как никогда в самых различных сегментах ТЭК. Так, например, массовый характер приобрело мошенничество на АЗС: на нашем счету на сегодняшний день уже десятки вскрытых схем, с помощью которых недобросовестные сотрудники обворовывают работодателя и клиентов АЗС из числа обычных водителей. Более того, ежемесячно этот "рейтинг" мошеннических комбинаций пополняется, как минимум, еще одной–двумя новинками. В среднем в зависимости от региона, прямые и косвенные потери на 100 заправочных станциях в квартал составляют до 40 млн руб.

Появился "черный" рынок софта и технических средств, позволяющих злоумышленникам скрыто вмешиваться в работу АСУ, подменять данные и т.д. Самые распространенные способы воровства на АЗС – хищения при совершении технических операций, неоплаченный налив, хищения при реализации, нарушение функционирования механизмов топливораздаточных колонок, мошенничество с бонусными картами. Мошенничают и воруют также при бункеровке, транспортировке и наливе нефтепродуктов. Но самые большие объемы кражи все же фиксируются при их переработке.

Внедрение (а главное – использование) механизмов и средств борьбы с мошенничеством позволяют избегать этих потерь и вовремя пресекать возникновение новых. Для большей эффективности необходимо сформировать и внедрить комплекс организационных и технических мер, который будет обеспечивать сбор и преобразование разнородных данных из различных систем, автоматическую обработку собранных данных с целью выявления фактов и признаков мошенничества, управление процессом расследования инцидентов и оперативное на них реагирование.

Внедрять такую систему необходимо по всей вертикали компании (от центральных площадок, являющихся концентратором всех данных, до отдельных объектов и дочерних обществ). Это позволит контролировать весь путь движения нефтепродуктов от розницы до нефтедобычи и нефтепереработки. А также осуществлять контроль логистики и подрядных организаций.

При этом основная масса способов и схем, по которым происходит мошенничество и кража нефтепродуктов, вскрывается уже на второй–третий месяц от начала подобного проекта, а через четыре–пять месяцев комплекс эффективно выявляет новые фрод-схемы и оперативно реагирует на них. ●

SI – новая аббревиатура в ИБ

Анна Костина, *руководитель направления систем управления безопасностью Центра информационной безопасности компании "Инфосистемы Джет"*

"Видеть и делать новое – очень большое удовольствие..."
Вольтер

За последние год – полтора в ИБ-сообществе практически прижилось понятие Security Intelligence (SI). Поверхностный анализ его употребления показывает, что чаще всего оно упоминается производителями систем обеспечения ИБ. Но при этом оказывается, что единого толкования термин пока не имеет. Что же все-таки кроется за этим понятием? Станет ли аббревиатура SI столь же привычной для специалистов в области ИБ, как, например, SIEM, DLP и другие? А если да, то что Security Intelligence им даст?

Security Intelligence весьма созвучно с давно устоявшимся понятием Business Intelligence, которое подразумевает инструменты и технологии сбора и преобразования данных из разнородных источников в значимую и полезную для целей бизнес-анализа информацию. Можно сделать вывод, что понятие SI также касается анализа данных, но уже в сфере безопасности. За счет возникновения все новых угроз стандартный набор систем обеспечения ИБ ежегодно увеличивается. Поэтому в сфере ИБ нет недостатка в данных, которые нужно анализировать.

Взгляд, устремленный вглубь или все-таки вширь?

По сути, данные можно анализировать в двух направлениях: вглубь и вширь. В первом варианте анализируются более детальные данные от систем обеспечения ИБ, причинно-следственные связи и взаимосвязи между событиями, уязвимости, которые привели к реализации событий ИБ. И здесь обычно речь идет о технических данных. В этом случае самый подходящий источник данных для анализа – системы мониторинга событий ИБ (SIEM). В них, как правило, уже подключены имеющиеся элементы инфраструктуры, имеющиеся системы обеспечения ИБ. И дело только за более детальной обработкой данных, поступающих в SIEM. И действительно, производители SIEM начали добавлять сочетание Security Intelligence к названиям своих продуктов, наделив свои SIEM дополнительными аналитическими функциями. А основные потребители таких данных, безусловно, – аналитики в области ИБ.

Если говорить об анализе данных вширь, то тут, в отличие от предыдущего примера, можно попытаться удовлетворить потребности руководителей ИБ-подразделений, а не только ИБ-аналитиков. Все те же данные, поступающие от систем обеспечения ИБ, можно анализировать не на техническом уровне, а в совокупности и более высокоуровнево. Что необходимо, например, при оценке эффективности тех или иных проведенных мероприятий или при отслеживании как трендов и изменений в состоянии ИБ внутри, так и изменений внешних угроз? Или, как вариант, при анализе ситуации и состояния ИБ в филиалах при территориально распределенной структуре или оценке достижения целей и задач в области ИБ, выполнения проектов, направленных на достижение целей ИБ? Иными словами, такой подход обеспечит поддержку принятия решений руководителями в области ИБ, поможет им держать руку на пульсе, своевременно определять проблемные области и реагировать на выявленные отклонения, не погружаясь без необходимости в детальные данные систем обеспечения ИБ.

Security Intelligence: истина меж двух крайностей

Оба варианта являются в некотором роде крайностями: одна – анализ глубоких технических данных, зачастую понятных узкому кругу специалистов; другая – анализ высокоуровневых и бизнес-ориентированных данных об ИБ. Причем оба варианта хороши и полезны, но между ними есть явный разрыв. Поэтому при развитии понятия Security Intelligence хотелось бы достичь некоторого баланса. С одной стороны, обеспечить сбор и анализ технических данных, с другой – иметь возможность эти же данные анализировать на более высоком уровне и желательно в интерфейсе одной системы (или нескольких, связанных между собой), чтобы переход от данных низкого уровня к данным высокого уровня был прозрачным для конечного их потребителя. Тем более, возвращаясь к изначальной аналогии с системами класса Business Intelligence, стоит вспомнить, что они-то как раз позволяют в рамках своего интерфейса представлять одни и те же данные "под разными соусами" и с каким угодно уровнем детализации. Именно эти задачи только начинают решаться в подходах к анализу данных о состоянии ИБ и процессах ее обеспечения. Все это приводит к созданию новых аналитических ИБ-систем и расширению понятия SI, заданного производителями SIEM-систем. Именно они представляют данные о состоянии ИБ в новом свете и дают возможность анализа эффективности процессов ИБ, связей и влияния их на бизнес, делают безопасность прозрачнее для более широкого круга заинтересованных сторон. ●

С течением времени (как это было с DLP, SIEM и др.) понятие Security Intelligence окончательно сформируется. Уже сейчас очевидно, что задач в области аналитики ИБ много, а значит, в ответ на эти вызовы будут развиваться аналитические системы, и аббревиатура SI прочно войдет в обиход специалистов в области информационной безопасности.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Что ждать от высоких технологий

Компания McAfee, подразделение Intel Security, опубликовала результаты исследования “Safeguarding 2025”, в котором приняло участие более 8000 человек по всему миру. В результате аналитики узнали основные ожидания потребителей от того, как изменятся их дома, рабочие места, автомобили, одежда и мобильные устройства. Кроме того, удалось выявить, что люди думают о том, как они смогут сохранять онлайн-безопасность и конфиденциальность, если количество техники значительно увеличится.

Количественная методика исследования

MSI Research провела онлайн-опрос среди 8094 человек в 12 странах в возрасте от 21 до 65. Участники опроса были распределены равномерно по возрасту и полу.

Опрос проводился с 1 по 12 августа 2014 г. в США, Великобритании, Германии, Нидерландах, Франции, Испании, Италии, Канаде, Бразилии, Мексике, Японии и Индии.

Потребители считают, что в ближайшее десятилетие технологии и устройства значительно изменят привычные принципы ведения домашнего хозяйства. Более половины (56%) участников верят, что через 11 лет появятся дома, которые смогут "говорить" или "читать". Более 68% полагают, что в будущем их холодильники смогут контролировать объем содержащихся в них продуктов и автоматически добавлять в список покупок необходимые позиции. Большинство респондентов (82%) уверены в том, что через несколько лет их системы охраны дома подключат к мобильным устройствам.

Исследование "Safeguarding 2025" выявило, что потребители понимают необходимость улучшения систем ИБ в связи с развитием носимых устройств и транспортных средств в 2025 г.

Платите с помощью телефона... или отпечатка пальца

29% считают, что они смогут оплачивать свои покупки с помощью отпечатка пальца, а 23% надеются, что они смогут делать это с помощью мобильного устройства. Одна пятая участников (21%) планирует по-прежнему использовать для этого кредитные карты.

Информационная безопасность

Согласно исследованию, 63% участников опроса озабочены тем, насколько хорошо будут развиты технологии обеспечения ИБ через 11 лет. Почти две трети респондентов (60%) заявили о том, что наиболее важными вопросами являются кража персональных данных, хищение денежных средств и мошенничество. И это неудивительно, так как практически каждый день публикуются новости о взломе цифровых систем розничных сетей и финансовых организаций. Потребителям предлагаются все новые и новые решения с расширенными сетевыми возможностями. Но многие по-прежнему испытывают чувство неуверенности при обмене персональной информацией или внедрении таких технологий, поскольку боятся стать жертвой киберпреступников.

Киберпреступность

Исследование также выявило, что 73% опрошенных боятся того, что в ближайшие десять лет члены их семей могут пострадать от действий хакеров. Более половины (54%) считают, что в 2025 г. их семьи могут стать жертвами кибербуллинга. По мере увеличения количества социальных сетей и их участников возрастает вероятность того, что пользователи ресурсов сети Интернет могут столкнуться с неприятностями.

Носимые устройства

68% участников опроса считают, что через 11 лет самым распространенным устройством будут "умные" часы, а 57% полагают, что носимые устройства получат широкое распространение. Более половины (57%) респондентов думают, что в домах будущего появятся кухонные приборы с подключением к сети Интернет.

Цифровые технологии на рабочих местах

В ближайшие 10 лет потребители ожидают увидеть значительные изменения, связанные с организацией их рабочих мест. Каждый четвертый (26%) считает, что он будет работать удаленно из дома, а 74% предполагают появление роботов и систем с искусственным интеллектом, которые начнут помогать им в работе. 66% верят в то, что они смогут получать доступ к данным с помощью технологий распознавания голоса или черт лица. И чем более вероятным это становится, тем более серьезные меры предосторожности необходимо предпринять для защиты конфиденциальной информации. Появление большего количества роботов на рабочих местах приводит, в свою очередь, к тому, что опасность киберпреступлений существенно увеличивается.

Защищайте ваше цифровое имущество

42% участников опроса считают, что к 2025 г. они смогут разблокировать свои устройства с помощью сканирования сетчатки глаза, а 31% предполагает, что эта операция будет выполняться путем сканирования отпечатка пальца. Практически все респонденты (89%) после принятия участия в опросе планируют в будущем предпринять меры для усиления защиты своих цифровых устройств.

"Зеленые" транспортные средства

35% участников опроса думают, что в 2025 г. они будут передвигаться с помощью гибридных транспортных устройств или самоуправляемых автомобилей (21%). Более двух третей респондентов (68%) считают, что в 2025 г. появятся автомобили с полностью автоматизированным управлением.

Ваши приложения будут контролировать состояние вашего здоровья

68% считают, что носимые устройства будут передавать данные о состоянии здоровья непосредственно лечащему врачу, что позволит отказаться от необходимости посещения больницы. Более трети (36%) участников считают, что будут существовать онлайн-системы проверки состояния здоровья с датчиками, прикрепленными к телу человека.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

10 ключевых правил для безопасности вашей сети

Стефан Винсот, *директор по маркетингу решений в области идентификации и доступа к информации компании Gemalto*

Чтобы корпоративные данные компании оставались в безопасности, нужно, прежде всего, позаботиться о безопасности корпоративной сети. Для этого необходимо соблюдать всего 10 ключевых правил.

Тенденции сетевой безопасности*

В течение 2014 г. успешные атаки были проведены на 80% компаний.

50% обнаруженных атак велись из внешних источников, 38% – от сотрудников компаний, 22% – от контрагентов.

Нарушения безопасности в основном возникали на рабочих станциях (44%) или ноутбуках сотрудников компании (26%). Причиной 16% атак стали смартфоны и планшеты сотрудников.

Наиболее серьезными последствиями кибератак опрошенные считают хищения информационных активов (45%), прерывание бизнес-процессов (44%) и санкции со стороны регуляторов (27%).

Компании направляют свои основные усилия в области сетевой безопасности на предотвращение сетевых атак. Наиболее популярные сетевые устройства: Firewall/VPN, защищенные маршрутизаторы и IDS/IPS-устройства. Наиболее популярные решения для конечных точек: антивирусы, anti-malware-программы и антиспам.

Исследование института Ponemon, при поддержке компании Juniper Networks

* В опросе приняли участие 1406 IT- и ИБ-специалистов Великобритании, Франции и Германии.

Резидентные модули OCR в хостовых DLP-системах: новый уровень защиты от утечек данных*

Сергей Вахонин, директор по решениям ЗАО "Смарт Лайн Инк"

Последние 3–4 года экосистема безопасности корпоративных IT, включая отрасль и рынок, переживает углубляющийся кризис, порожденный, с одной стороны, коммерциализацией киберпреступности и усилением фактора геополитизации, а с другой – замедлением идеологического и технологического развития систем защиты данных. Факторы эти усиливают друг друга, порождая кумулятивный негативный эффект, заметно нарушающий динамический баланс между угрозами корпоративной ИБ и средствами ее обеспечения – причем не в пользу последних.

Удивительно, но каждый очередной год отраслевые аналитики и эксперты в области ИБ провозглашают "годом утечек данных", и это уже никому не кажется феноменальным. Вот и нынешний, 2014 г. уже стал новым абсолютным чемпионом в этой гонке, несмотря на то, что "бежать" предстоит еще квартал – благодаря невиданным доселе по масштабам и последствиям утечкам данных клиентов американской розничной сети Target и ее земляка, онлайн-ритейлера eBay.

Очевидно, что инциденты, связанные с утечками данных, следует разделять на две группы – вызванные внешними атаками и "внутренние" инсайдерские утечки. Существенную часть инцидентов, связанных с внешними атаками, можно предотвратить применением средств защиты компьютеров от заражения вредоносным ПО (вирусами, троянами, APT). Для борьбы с инсайдерскими утечками из корпоративных ИС наиболее эффективными компонентами являются специализированные системы защиты – так называемые data leak prevention, или DLP-системы. Они позволяют блокировать не субъект или первопричину утечки (вредоносное ПО или действия инсайдера), а непосредственно ее саму, например, отсылку конфиденциального документа по личной электронной почте или его выгрузку на сайт социальной сети. Применение DLP-систем в любом случае необходимо потому, что угрозы утечек создаются не только и не столько хакерскими атаками извне, сколько обычными работниками предприятия – невольно, по халатности или злому умыслу.

Оружие современных DLP-систем

Основным "оружием" всех современных DLP-систем являются технологии контентного анализа и фильтрации, позволяющие выявлять в текстах документов, файлов, писем, вложений и прочих объектов данные, запрещенные политикой ИБ, и блокировать операции по их передаче за пределы компьютера или сети организации, будь то печать на принтере, запись на флешку, передача по Skype, почте и т.д. Именно на таких технологиях производители DLP-систем делают основной акцент, усиленно развивая и совершенствуя методы контентного анализа, причем порой в ущерб фундаментальным контекстным механизмам контроля и предотвращения утечки. В качестве примеров прогрессивных технологий можно привести морфологический анализ, поддержку и развитые заготовки шаблонов регулярных выражений, детектирование комбинаций ключевых слов с поддержкой промышленных и отраслевых словарей, цифровые отпечатки документов и пр. Можно утверждать, что сегодня в целом достигнут достаточно высокий уровень надежности и эффективности детектирования и фильтрации текстового контента.

Явные минусы

Однако до сих пор ни в одной из доступных на российском рынке DLP-систем не был достаточно надежно перекрыт такой простой и доступный даже неопытным пользователям ПК прием обхода контентной защиты, как конвертация текстовых данных в графические изображения, к которым методы анализа текстовых форматов принципиально не применимы. Причем пользователи вовсе не обязательно конвертируют текст в графику со злым умыслом – нормальной бизнес-практикой является пересылка сканированных документов, причем как в форме графических файлов, так и после конвертации в PDF, а также в виде вложений в обычные документы MS Office или электронные сообщения.

Конечно же, этот недостаток, равно как и средство его устранения, не являются секретом. Ряд российских и зарубежных разработчиков DLP-систем уже в той или иной форме использует в своих продуктах технологии обратной конвертации графики в текст (Optical Character Recognition), интегрируя OCR-модули в DLP-системы. К сожалению, в силу обусловленных историческими причинами дорого-

визны и "тяжеловесности" OCR-модулей их применение в современных DLP-системах ограничено, как правило, DLP-шлюзами или DLP-серверами, то есть от утечек данных в графической форме защищается только офисная сеть и только при их передаче по сетевым каналам связи. При этом исходящие коммуникации ноутбуков и лэптопов сотрудников при их работе из-за пределов корпоративной сети – например, в командировке или дома – принципиально не контролируемы OCR-модулями DLP-шлюзов. Кроме того, реализационные ограничения OCR-компонентов многих существующих DLP-систем позволяют анализировать только файлы графических форматов, но не изображения, встроенные в офисные документы. В результате остается полностью открытым такой примитивный и общедоступный канал утечки данных, как "вставить скан документа в Word и отослать по почте". Еще одним неконтролируемым сценарием утечки информации является копирование графических данных с ПК на съемные накопители или их печать на локальных принтерах, поскольку для этих типов операций перехват и пересылка проверяемой графики для анализа на DLP-сервер в реальном масштабе практически нереализуемы.

Решение есть!

Именно на разработку OCR-компонента, свободного от всех перечисленных недостатков, и его интеграцию в свое DLP-решение сфокусировала усилия компания "Смарт Лайн". Уже в ближайшее время на рынке появится его новая версия DeviceLock DLP 8, исполнительные агенты которого оснащены резидентным OCR-модулем, обеспечивающим распознавание графических образов текста в изображениях как в виде файлов графических форматов, так и встроенных в документы. При попытке передачи пользователем данных и файлов по сетевым каналам, их печати или копирования на устройства хранения DeviceLock DLP в соответствии с заданными DLP-политиками применяет OCR-технологии для анализа, детектирования и фильтрации графических образов конфиденциальных текстовых данных в сканах документов, снимках экранов и изображениях внутри офисных документов.

Важно подчеркнуть, что OCR-модуль DeviceLock DLP является резидентным, встроенным в агент, который, в свою очередь, устанавливается на всех контролируемых компьютерах и обеспечивает инспекцию и протоколирование приложений, использующих как сетевые каналы, причем независимо от используемых ими портов и способа выхода в Интернет, так и локальные периферийные устройства. Принципиальным преимуществом такой архитектуры является реализация защитных действий по блокировке и протоколированию почтовых отправлений, переписки и передачи файлов в социальных сетях и через службы мгновенных сообщений, в том числе содержащих данные в графическом формате, в момент отправки данных по сети "на лету" непосредственно на рабочем компьютере сотрудника – будь то офисная рабочая станция, лэптоп вне корпоративной сети или даже BYOD-устройство в терминальной среде. В результате работоспособность DLP-системы DeviceLock в целом и OCR-компонента в частности никак не зависит от доступности корпоративной сети или подключения к серверам, что позволяет службам ИБ обеспечить безопасность почтовых коммуникаций сотрудников даже в условиях, когда их бизнес-функции требуют мобильности.

Другой пример практического использования резидентного OCR-модуля и архитектурных особенностей DeviceLock DLP – контроль данных, в том числе в графическом формате, в распределенной корпоративной среде, когда организация располагает широкой сетью филиалов и подразделений, что делает нерациональным использование DLP-серверов в массе либо в силу малочисленности филиалов, либо вследствие недостаточной пропускной способности сети передачи данных. К примеру, DeviceLock DLP 8 можно применить для защиты от утечек экзаменационных материалов ЕГЭ, распространяемых в графической форме и используемых в тысячах образовательных учреждений, зачастую не имеющих достаточно "быстрых" каналов связи для "внешнего" анализа данных на DLP-серверах.

OCR-технологии, применяемые в агентах DeviceLock для защиты обычных и виртуальных рабочих сред, позволяют как уменьшить информационные риски, так и обеспечить неукоснительное исполнение сотрудниками политик безопасности внутри и за пределами компании. Помимо DLP-агентов OCR-технологии используются в новом компоненте комплекса – DeviceLock Discovery, – предназначенном для сканирования компьютеров пользователей, сетевых каталогов и систем хранения данных с целью выявления и устранения нарушений политик безопасного хранения данных.

DeviceLock Discovery реализует сканирование и обнаружение данных двумя способами – как удаленно с сервера Discovery, так и непосредственно на рабочих станциях с агента Discovery (который, в свою очередь, может быть как установлен на компьютер при необходимости сервером, так и встроен в агент DeviceLock). Оптическое распознавание текста в изображениях, встроенных в документы, или в графических файлах, хранимых на жестких дисках рабочих станций и сетевых устройствах, выполняется при сканировании любым из этих способов – OCR-модуль в DeviceLock присутствует и в серверной вариации, и на агентах.

Стоит также отметить, что использование OCR-технологий в DeviceLock не потребует дополнительных финансовых затрат клиентов – данный функционал отдельно не лицензируется.

Релиз-кандидат DeviceLock DLP 8 уже доступен для ознакомления на Web-сайте **www.devicelock.com.**

Периметр в облаке – он есть или его нет?

Владимир Воротников, *руководитель отдела перспективных исследований и проектов ЗАО "С-Терра СиЭсПи"*

К понятию облачных технологий сейчас относят зачастую избыточное количество технологий. Как следствие, количество новой терминологии зашкаливает, и к тому же она далеко не всегда согласована между различными вендорами. Это не способствует пониманию происходящего у рядовых администраторов и инженеров. Непонимание, как любая неопределенность, вызывает тревогу и страх.

За облаками всегда скрывается солнце

Одной из популярных тем, активно обсуждаемых в последнее время в IT-сообществе, является безопасность облачных сред. Некоторые предпосылки к таким активным обсуждениям очевидны. С одной стороны, в облачных технологиях возникает большое число новых угроз, с другой – сама суть облачных технологий подразумевает консолидацию большого количества информации и ресурсов в одном месте, что повышает ответственность за их безопасность. Есть и менее очевидные предпосылки. Например, к понятию облачных технологий сейчас относят огромное, зачастую избыточное количество технологий. Как следствие, количество новой терминологии зашкаливает, и к тому же она далеко не всегда согласована между различными вендорами. Это не способствует пониманию происходящего у рядовых администраторов и инженеров. Непонимание, как любая неопределенность, вызывает тревогу и страх. А дальше действует положительная обратная связь: множественные статьи и обсуждения безопасности облаков вызывают ощущение непреодолимости и чудовищного масштаба проблемы, что вызывает еще больший страх. Мне бы хотелось приободрить коллег и напомнить, что за облаками всегда скрывается солнце.

Классический защищенный сегмент сети похож на средневековую крепость: стены крепкие, все входы и выходы известны, внутри – все свои, проверенные люди. Сегмент сети в облаке, в таком случае, больше похож на хостел: в вашей комнате какие-то незнакомые соседи, которые меняются каждый день. Двери вроде как запираются, но ключи от всех дверей есть у администрации, да еще и эту самую администрацию вы в лицо не знаете. Тревожное место.

Многовековая защита

Многие тысячелетия природа учила человека строить укрытия. Огородил вход в пещеру – внутри безопасно. Обнес замок высокой стеной – и чувствуешь себя защищенным. Неудивительно, что по тому же принципу человек начал строить защиту своих данных. Серверная – закрытое помещение, которое запирается на ключ, следовательно, физически данные защищены, можно быть спокойным. Есть только один выход для данных наружу – через канал провайдера, и он закрывается межсетевым экраном. Тут становится немного тревожнее. Подсознание, конечно, больше доверяет дверям и ключам, чем странному металлическому аппарату с проводами. Но паники пока не возникает. Все-таки защитника своих данных видно (вон он в стойке мигает лампочками) и его даже можно потрогать рукой. А если что – всегда можно взять и отрезать канал провайдера ножницами по металлу. Во избежание, так сказать.

Таким образом, человек вообще и инженер в частности всю свою жизнь привык огораживать ценные для себя вещи и данные реально осязаемыми системами защиты, принадлежащими только ему. Это четкое понимание наличия границы, или периметра, все входы и выходы из которого понятны, дает ощущение если не безопасности, то, по крайней мере, контролируемости ситуации.

Хостел или банк?

Совсем по-другому дела обстоят в случае применения облачных технологий. Больше нельзя понять, где конкретно находятся твои данные. Некоторые авторы утверждают, что периметр пропадает, но я с этим не соглашусь. Периметр остается. Но он, во-первых, становится динамическим, постоянно меняющимся, как и само пространство вашего контроля, которое постоянно меняется. Во-вторых, в периметре появляется намного больше дверей, причем большинство из них человек не в силах увидеть глазами и пощупать руками, их можно только осознать мозгом.

Здесь, мне кажется, уместна следующая аналогия. Классический защищенный сегмент сети похож на средневековую крепость: стены крепкие, все входы и выходы известны, внутри – все свои, проверенные люди. Сегмент сети в облаке, в таком случае, больше похож на хостел: в вашей комнате какие-то незнакомые соседи, которые меняются каждый день. Двери вроде как запираются, но ключи от всех дверей есть у администрации, да еще и эту самую администрацию вы в лицо не знаете. Тревожное место. Студенту переночевать – пойдет. Бизнесмену с кейсом денег – как-то не очень. Можно, конечно, снять отдельную комнату и закрыться там, но коридоры остаются общие с другими посетителями. И никто не даст гарантию, что в соседней комнате не устроят пожара или не будут кричать всю ночь под окнами. Да и ключи все еще есть у администратора. Еще один вариант – арендовать или выкупить весь хостел целиком. Что уже неплохо, но ряд проблем все равно придется решать. В этом примере легко просматриваются отсылки к разным типам (SaaS, PaaS, IaaS) облачных сервисов, а также частным и публичным облакам.

Еще один пример. В облаках мы не можем осуществлять самостоятельный контроль за сохранностью данных и должны передать эти полномочия другим людям. Напрашивается аналогия с банковскими депозитами. Мы можем сложить деньги под подушку или в чемоданчик с ключом – и при этом постоянно беспокоиться за них. Или же отдать на хранение в учреждение, предоставляющее гарантии сохранности денег, –

банк. Беспокоиться все равно будем, но безопасность наших сбережений в таком случае обеспечивается репутацией организации и государственными гарантиями, такими как Система страхования вкладов и регламенты СТО БР. Посмотрите вокруг, банки вошли в нашу жизнь, и их услугами пользуются все. Можно ожидать подобного и в области хранения и обработки информации. С течением времени операторы ЦОД выйдут на высокий уровень защищенности, заработают репутацию, а государственные органы выработают стандарты защиты (начало положено указами ФСТЭК по защите виртуализации, а также готовящимися к выходу ГОСТами по защите в облаках и по защите виртуализации). Возможно, хранить свои данные в облаке станет безопаснее, чем локально.

Несколько советов

Вернемся к периметру, а точнее, к той динамической структуре, в которую он превратился. Понятно, что в такой схеме невозможно осуществлять полный самостоятельный контроль своих постоянно меняющихся границ и приходится доверять внешнему управляющему, гипервизору, на которого ложится гигантская ответственность. И в целом нельзя сказать, что гипервизоры не готовы к ней. Да, периодически находятся новые уязвимости, но надо понимать, что уязвимости есть в абсолютно любой системе. Мы научились доверять автопилотам и бортовым системам в самолете свои жизни, нам придется научиться доверять гипервизорам свои данные.

Но это не значит, что мы ни на что не можем повлиять. Есть несколько общих моментов, которые необходимо учитывать.

Во-первых, не стоит впадать в паралич перфекциониста. "Если я не могу быть уверен, что данные из ОЗУ моей виртуальной машины не попадут в другую виртуальную машину, то они де-факто скомпрометированы и можно даже не пытаться их спасти", – в корне неправильная позиция. В ней нарушается один замечательный принцип: "убегая от медведя, не нужно бежать быстрее всех, важно бежать быстрее последнего". Следует всегда помнить, что многие атаки, хоть и возможны в теории, но на практике чрезвычайно сложны и могут потребовать серьезных ресурсов и высочайшей квалификации исполнителя. Никто в жизни не попытается атаковать гипервизор крупного хостинга ради ваших данных, если их можно получить через тривиальную SQL-инъекцию на вашем сайте. Поэтому закройте потенциальные уязвимости адекватно стоимости своих данных. Естественно, что чем больше стоят данные, тем более надежную и контролируемую инфраструктуру придется выбрать. Да, не секрет, что построение собственного частного облака может оказаться дороже использования своего существующего публичного аналога. Но во все времена более высокий уровень защиты приводил к большим затратам.

Во-вторых, помогите защитить свои данные гипервизору тем, чем можете. Закройте часть входов в периметр самостоятельно. Шифруйте данные, записываемые на диск. Это снизит риск их компрометации. Шифруйте данные, выходящие через сетевые интерфейсы ваших устройств. Это чрезвычайно важно: огромный набор различных сетевых атак вам больше не страшен. Обеспечьте защищенный доступ к своим данным извне. На рынке сейчас существует ряд продуктов по шифрованию и межсетевому экранированию, в том числе в виртуализированных средах. Надо сказать, что если раньше подобная защита была доступна только у западных вендоров, то сейчас появились и отечественные разработки, полностью отвечающие требованиям регулятора в области защиты персональных данных.

Резюмируя все вышесказанное

Еще раз обратим внимание: периметр – не исчез. Но он трансформировался в более сложную сущность, которую человек не в силах контролировать напрямую в реальном времени, и в вопросах его защиты приходится полагаться на соответствующие инструменты. В этом нет ничего страшного, но поскольку на данном этапе данные инструменты находятся в начале своего долгого пути, следует не забывать и о традиционных методах защиты, которые не менее важны. ●

Комментарий эксперта

Антон Шкарин,
руководитель группы разработки продукта "Гарда Предприятие", компания "МФИ Софт"

Как защитить DLP-систему от атак?

Большинство современных DLP-систем построены на основе клиент-серверной архитектуры. Как правило, хранение и обработка информации (в том числе и конфиденциальных данных) осуществляется именно на сервере. Клиент же представляет собой "тонкое" приложение с логикой, ограниченной обменом информацией с сервером и визуализацией полученных от сервера данных.

Поэтому и защиту DLP-системы можно разделить на несколько уровней:

1. Защита сервера;
2. Защита клиента;
3. Защита канала между сервером и клиентом.

Хорошим подходом к обеспечению безопасности сервера является, в первую очередь, изоляция его от внешнего мира, в том числе, от прямого доступа из Интернета (сервер находится в отдельной локальной подсети). Эта достаточно просто реализуемая мера сильно осложнит проведение атак на сервер DLP-системы хакерами. Далее следует позаботиться об организации хранения данных на сервере. Если доступ к ней был все-таки получен, шифрация данных на жестких дисках или своя файловая система делают трудозатраты по приведению такой информации к читаемому виду (по сути, декодированию) настолько большими, что сроки и стоимость выполнения такой работы могут превышать сроки актуальности самой информации, хранящейся на сервере DLP.

Защита клиента сводится к реализации системы управления доступом и разграничения прав (дискреционная, ролевая или мандатная модель), включающей в себя аутентификацию пользователей (вход по логину/паролю + дополнительные ограничения на сложность пароля, время его жизни, количество неверно введенных пар логин-пароль и прочие механизмы). В дополнение к этому действия каждого оператора DLP-системы необходимо логировать, чтобы защитить систему от одного из худших случаев, когда оператор является нарушителем информационной безопасности. Данное средство позволит руководителю отдела ИБ (или сотруднику, на которого возложены такие обязанности) выявлять недобросовестных пользователей DLP-системы.

Для обеспечения защиты канала связи между сервером и клиентом стандартом де-факто стало использование криптографических протоколов SSL или TLS, которые предотвращают возможность прослушивания канала.

Совокупность вышеописанных мер делает DLP-систему хорошо защищенной от хакерских атак и недобросовестных операторов. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Удаленный доступ и утечка данных

Сергей Вахонин, *директор по решениям, ЗАО "Смарт Лайн Инк"*

Предоставление доступа к информационным активам компании через удаленное подключение является одним из наиболее перспективных направлений развития информационных систем. Помимо преимуществ, вытекающих из мобилизации сотрудников, очевидны также и проблемные зоны — прежде всего это безопасность данных, доступных при удаленном доступе.

Немного статистики

Согласно статистическим исследованиям, более 40% сотрудников работают удаленно хотя бы один день в неделю. По прогнозам Gartner, более 38% рабочих процессов будет выполняться с помощью BYOD-устройств, хотя на сегодня эта доля составляет всего порядка 6%. При этом 52% российских компаний игнорирует вопросы мобильной безопасности и никаким образом не контролирует доступ к корпоративным сервисам и файлам с личных планшетов и смартфонов сотрудников.

Нет никаких сомнений в том, что прогноз Gartner по BYOD сбудется, и вскоре мобильной станет значительная часть работников, равно как и начнет расти доля сотрудников, работающих с применением личных компьютеров в модели "домашнего офиса". Остановить эти процессы не только невозможно, но и контрпродуктивно для бизнеса – использование персональных устройств, как правило, повышает работоспособность и производительность труда сотрудников, облегчает их мобильность, упрощает возможность практического использования корпоративных данных в различных ситуациях.

Сама практика хранения данных на BYOD-устройствах порождает риск неконтролируемой утечки данных, независимо от наличия на устройстве агента MDM-системы. Данные ограниченного доступа могут быть попросту отправлены непосредственно с мобильного устройства по сетевым каналам (почта, социальные сети, мессенджеры и др.) или на подключаемые внешние устройства печати и хранения данных.

В ряде бизнес-сценариев будет предпочтительнее использовать именно MDM-системы для защиты данных на мобильных устройствах, например, когда сотруднику "в поле" потребуется иметь доступ к корпоративным данным вследствие низкой пропускной способности канала или полного отсутствия сетевого подключения, а значит, должна быть возможность защищенно хранить корпоративные данные локально на персональных мобильных устройствах.
Если же проблем с доступом в сеть нет или сотрудник пользуется полноценным компьютером в домашних условиях, Virtual DLP будет оптимальным решением.

Это означает, что многие компании поставлены перед необходимостью искать разумный баланс между мобильностью сотрудников и информационной безопасностью бизнеса, решая ряд новых задач, связанных с эффективностью управления персональными устройствами и обеспечением безопасности их применения.

Прежде чем приступить к решению задачи предоставления удаленного доступа к корпоративным ИС, следует определиться с ответом на вопрос – допустима ли обработка конфиденциальных данных компании на личных компьютерах и мобильных устройствах?

Скорее всего, большинство компаний ответит "Да", следуя современному тренду развития мобилизации. При этом службам ИБ потребуется решить задачу контроля корпоративных данных, передаваемых и хранимых на персональных устройствах, то есть явно прописать требования по использованию мобильных устройств (корпоративных и личных) и удаленного доступа к корпоративным ресурсам и сервисам, повысить уровень осведомленности сотрудников и, разумеется, внедрить специализированные средства управления мобильными устройствами и защиты данных.

Для решения таких задач безопасности персональных устройств, и в особенности BYOD-устройств, рынок предлагает множество самых разных средств и систем.

Mobile Device Management

Системы класса Mobile Device Management (MDM) позволяют удаленно (централизованно) управлять множеством мобильных устройств, будь то устройства, предоставленные сотрудникам компанией, или собственные устройства сотрудников. Сильными сторонами MDM-систем являются такие функции, как надежная парольная защита устройства, шифрование встроенной памяти и карт хранения данных, либо "контейнеризация" данных приложений, управляемое уничтожение данных с устройства в случае потери или кражи. Однако же на практике, по крайней мере, функцию удаленного уничтожения данных можно реализовать только при условии, что устройство появится в сети и будет обнаружено управляющей частью MDM-системы, то есть приходится полагаться на удачу или низкую техническую квалификацию вора или человека, нашедшего такое "защищенное" мобильное устройство, и на то, что при этом корректно сработают функции шифрования и парольной защиты.

Стоит также помнить, что уже сама практика хранения данных на BYOD-устройствах порождает риск неконтролируемой утечки данных, независимо от наличия на устройстве агента MDM-системы. Данные ограниченного

доступа могут быть попросту отправлены непосредственно с мобильного устройства по сетевым каналам (почта, социальные сети, мессенджеры и др.) или на подключаемые внешние устройства печати и хранения данных.

Virtual DLP

Другим эффективным и перспективным решением для обеспечения безопасности данных при использовании персональных устройств является предоставление удаленного доступа к информационным активам компании через терминальные сессии, когда виртуальные или физические рабочие Windows-среды защищены функционирующей на хосте, а не на BYOD-устройстве, DLP-системой. Такой подход называется Virtual Data Leak Prevention (Virtual DLP). Коротко говоря, технология Virtual DLP предлагает контролируемое предоставление удаленного доступа к корпоративным данным в отличие от локального хранения данных на BYOD-устройствах в подходе MDM.

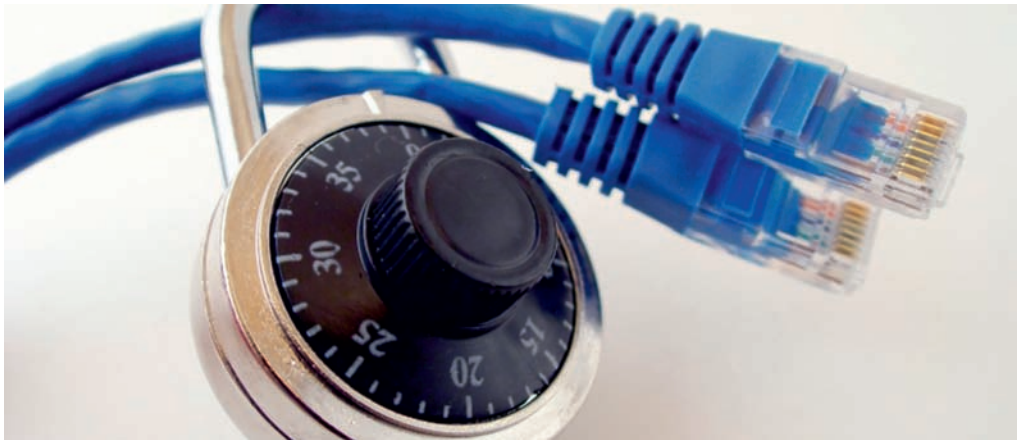
Концепция Virtual DLP подразумевает выполнение ключевых задач безопасности:

- безопасная обработка данных – для обработки корпоративной информации используются приложения, опубликованные в виртуальной среде;
- безопасное хранение данных – защищаемые корпоративные данные могут быть доступны только в виртуальной среде на время работы с ними, могут сохраняться только на сервере;
- контроль передачи данных – DLP-система обеспечивает контентную фильтрацию содержимого файлов и данных, проходящих через коммуникационные каналы, и избирательный контроль каналов передачи и хранения данных (электронная почта, веб-сайты, мессенджеры и т.д., канал печати, перенаправленные диски и сетевые файловые ресурсы, съемные носители).

Стоит отдельно предостеречь от вывода, что MDM-решения не нужны или бесполезны, раз есть DLP-системы, обеспечивающие контроль данных при удаленном доступе. В ряде бизнес-сценариев будет предпочтительнее использовать именно MDM-системы для защиты данных на мобильных устройствах, например, когда сотруднику "в поле" потребуется иметь доступ к корпоративным данным вследствие низкой пропускной способности канала (нет LTE/3G) или полного отсутствия сетевого подключения (например, в самолете), а значит, должна быть возможность защищенно хранить корпоративные данные локально на персональных мобильных устройствах. Если же проблем с доступом в сеть нет или сотрудник пользуется полноценным компьютером в домашних условиях, Virtual DLP будет оптимальным решением.

"Полная" модель Virtual DLP, предлагающая всеобъемлющую стратегию безопасности удаленного доступа к корпоративным ресурсам, подразумевает применение в комплексе MDM-системы для контроля локальных приложений на устройствах, удаленного уничтожения данных, обеспечения надежной парольной защиты устройства и шифрования данных и т.п., защищенного VPN-туннеля, и, наконец, DLP-системы для предотвращения утечек данных с персонального устройства.

По большому счету, модель Virtual DLP является идеальным вариантом обеспечения безопасности со многих точек зрения – ведь, по сути, это предоставление пользователю стерильной рабочей среды, созданной IT-службой без вмешательства или участия пользователя. Такая среда содержит те и только те бизнес-инструменты, которые необходимы пользователю для его служебных задач – от полноценной Windows-среды в форме виртуальной или физической машины (рабочего стола) до отдельного опубликованного приложения, доступ к которым пользователь получает через терминальную сессию. Одним из преимуществ виртуализации является тот аспект, что пользователь может получить защищенный удаленный доступ к корпоративной среде с помощью любого типа компьютеров и персональных устройств – тонкий клиент, лэптоп, планшет, смартфон. Все, что нужно сотруднику, – это клиент для удаленного доступа по протоколу RDP или ICA (например, Citrix Receiver), или же в качестве терминального клиента может использоваться любой Web-браузер, поддерживающий HTML5. ●



Согласно статистическим исследованиям, более 40% сотрудников работают удаленно хотя бы один день в неделю. По прогнозам Gartner, более 38% рабочих процессов будет выполняться с помощью BYOD-устройств, хотя на сегодня эта доля составляет всего порядка 6%. При этом 52% российских компаний игнорирует вопросы мобильной безопасности и никаким образом не контролирует доступ к корпоративным сервисам и файлам с личных планшетов и смартфонов сотрудников.

Многие компании поставлены перед необходимостью искать разумный баланс между мобильностью сотрудников и информационной безопасностью бизнеса, решая ряд новых задач, связанных с эффективностью управления персональными устройствами и обеспечением безопасности их применения.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

К вопросу обнаружения компьютерных атак и вредоносного заражения

Александр Грибков, *главный конструктор системы*
Виталий Багликов, *главный конструктор по информационной безопасности*
Валерий Иващенко, *генеральный директор*
ООО "КБПМ – информационная безопасность"

С каждым годом нарастающие угрозы компьютерных атак и вирусного заражения информационных систем предприятия требуют постоянного совершенствования технологии обеспечения информационной безопасности в части создания многоэтапной системы защиты информационно-вычислительных систем.

Несмотря на разработку альтернативных методов обнаружения компьютерных атак и вредоносного программного обеспечения, сигнатурный метод поиска в настоящее время остается основным в решении задачи обеспечения информационной безопасности ЛВС, подключенных к Интернету.

В настоящее время используются две основные схемы применения систем обнаружения атак (СОА) и антивирусных средств (АВС). В распределенных системах применения СОА и АВС устанавливаются непосредственно на защищаемые серверы и рабочие станции. Достоинством такой схемы будет то, что АВС обнаруживают компьютерные вирусы независимо от источника заражения, недостаток заключается в необходимости организовать в ЛВС централизованное обновление без сигнатур.

Рис. 1. Комплекс аппаратных средств ПАС "Сенсор"

В сосредоточенных системах применения СОА и АВС устанавливаются на отдельные программно-аппаратные комплексы (ПАК) в каналах связи с внешними сетями, чаще всего в каналах связи с сетью Интернет. Эти ПАК осуществляют поиск в трафике канала сигнатур компьютерных атак и компьютерных вирусов (являются сенсорами КА и КВ). Такая схема удобна, когда единственным источником информации в ЛВС служат внешние сети. Если получение информации осуществляется через отчуждаемые носители, ПАК обнаружения КА и КВ дополняется комплексом обнаружения вредоносного ПО на отчуждаемых носителях.

Защита корпоративной ЛВС

Перспективным вариантом применения защиты каналов связи является защита корпоративной ЛВС в целом, особенно если это ЛВС с пространственным разнесением сегментов. В этом случае целесообразно на каналах связи сегментов корпоративной ЛВС разместить сенсоры КА и КВ, которые для централизованного хранения информации, аналитической обработки и управления процессом поиска желательно дополнить корпоративным центром обработки переданных сенсорами данных о КА и КВ.

Для решения задачи обнаружения КА и КВ в корпоративных ЛВС применима новая разработка нашей организации – программно-аппаратная система (ПАС) "Сенсор", способная выявлять скрытые угрозы в трафике каналов связи. Другой разработкой является ПАК "Пункт-МС" (http://kbpm-ib.ru/punktms), способный обнаруживать КВ на отчуждаемых носителях информации различного типа.

Основными проблемами системы выявления сетевых атак и компьютерных вирусов являются:

- нарастающий объем трафика в ставших уже стандартом де-факто гигабитных сетях;
- своевременное обнаружение сетевых атак и компьютерных вирусов в трафике;
- оперативный сбор и анализ выявленной информации.

Применение

Исходя из имеющегося положительного опыта создания сенсоров, коллектив нашей организации поставил перед собой задачу – объединить в единой модульной ПАС систему обнаружения КВ с системой выявления КА. Данная система предназначается для:

- приема и контроля трафика для дальнейшего анализа по двум независимым потокам на скорости 1 Гбит/с без потерь сетевых пакетов;
- выявления вредоносного программного обеспечения (по фиксированному набору сетевых протоколов: HTTP, POP3, SMTP, FTP) и сетевых атак в режиме реального времени;
- систематизации информации от подсистем выявления вредоносного программного обеспечения и сетевых атак, ведения СУБД и формирования статистических характеристик анализируемого трафика;
- первичного экспресс-анализа факторов в выявленных атаках и вирусах.

Комплектация

Комплекс аппаратных средств состоит из нескольких подсистем, обеспечивающих выборку из сетевого трафика, сервера базы данных, хранящего отобранную и преобразованную информацию (см. рис. 1).

Модульная структура ПАС "Сенсор" позволяет использовать его как в полном составе, так и с исключением отдельных подсистем по выбору пользователя (см. рис. 2).

В состав ПАС входят следующие подсистемы:

- выявления сетевых атак ("Сенсор-Атака");
- выявления вредоносного ПО ("Сенсор-Вирус");
- передачи данных от подсистем "Сенсор-Атака" и "Сенсор-Вирус" в базу данных;
- модуль хранения данных;
- технологического мониторинга аппаратной части системы;
- визуализации и экспресс-анализа данных.

В ПАС могут использоваться различные комбинации из одной или нескольких подсистем выявления атак и выявления вредоносного ПО, которые являются прозрачными. Они получают доступ к сетевому трафику через зеркалирование

портов или через TAP-устройство. Захват данных на гигабитном канале обеспечивается с помощью высокоскоростной библиотеки захвата пакетов и специализированного драйвера сетевой карты.

В части обнаружения сетевых атак используется ставшее де-факто стандартом средство Snort, информация от которого в части выявленной атаки преобразуется в сообщение, являющееся информационным пакетом безопасности (ИПБ).

Диагностика

С целью обнаружения вложенных компьютерных вирусов из проходящего трафика производится сборка сессий, распознавание по нескольким популярным протоколам прикладного уровня и выделение переданных по ним объектов. Для диагностики на инфицированность все извлеченные файлы отправляются на проверку антивирусным средством Dr.Web (выбор обусловлен наличием сертификата безопасности и скоростными характеристиками). В случае обнаружения заражения выделенный из трафика файл сохраняется в специальный "контейнер" (для защиты от непреднамеренного запуска) и формируется сообщение в виде информационного пакета безопасности.

Сгенерированные подсистемами информационные пакеты передаются в единую базу данных. Передача осуществляется в клиент-серверном режиме с периодичной посылкой сигналов об отправке очередной порции сообщений. Для быстроты пересылки ИПБ, "контейнеров" и статистической информации от подсистемы "Сенсор-Вирус" используется сжатие передаваемых данных. Для гарантии передачи разработан протокол передачи и выполняется проверка контрольных сумм данных.

Подсистема передачи и отображения технологической информации о состоянии работоспособности подсистем реализована на основе свободной системы мониторинга ZABBIX.

Вся информация хранится в СУБД PostgreSQL.

Подсистема визуализации позволяет через дружественный web-интерфейс отображать статистическую информацию об обнаруженных КА и КВ, а также производить первичный экспресс-анализ выявленных фактов атак и вирусов.

Узким местом системы является выявление компьютерных вирусов. Антивирусное средство имеет ограниченную скорость проверки на наличие компьютерных вирусов. Имеющийся опыт обработки и анализа сетевого трафика по каналам связи производительностью 100 Мбит/с свидетельствует о том, что очередь файлов к антивирусному средству на проверку может накапливаться и даже расти. При снижении интенсивности притока файлов в очередь – как правило, в ночное время – разбор очереди иногда продолжается несколько часов.

Для анализа извлеченных из гигабитного канала данных требуется поддерживать скорость антивирусной проверки достаточно высокой. Есть несколько путей решения этой задачи.

Первый путь – одновременный запуск нескольких демонов антивирусного средства в зависимости от характеристик процессора. Оптимальной конфигурацией на определенном смоделированном трафике является запуск трех демонов антивирусного средства, при этом каждый обрабатывает 16 потоков. Данная конфигурация позволяет почти в два раза повысить скорость определения зараженности объектов (см. рис. 3).

Второй путь – использование агрегации файлов, посылаемых антивирусному средству, в tar-архивы оптимального размера, что сокращает время обработки.

Третий путь – наращивание производительности аппаратной платформы. Один из вариантов – использование платформы с независимыми вычислительными модулями в едином серверном шасси 2U с общей дисковой подсистемой.

Использование указанных путей в формировании программно-аппаратных систем позволяет создавать системы разной комплектации в зависимости от требуемого функционала с целью контроля интернет-трафика на наличие сетевых атак и вирусов.

Для обеспечения требований безопасности ПАС предусмотрена возможность разделения информационных контуров на "открытый" и "закрытый" с хранением и обработкой данных в "закрытом" контуре, не имеющем выхода во внешние сети. Связь между контурами может обеспечиваться сертифицированным однонаправленным оптическим

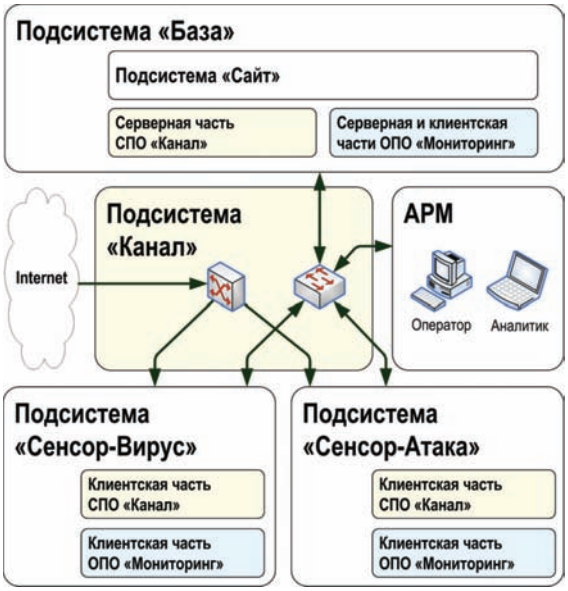


Рис. 2. Структурно-логическая модель ПАС "Сенсор"

Рис. 3. График изменения скорости работы Dr.Web

шлюзом (www.kbpm-ib.ru/odnsh). Возможна также организация криптозащиты канала передачи данных между удаленными сенсорами в "открытом" контуре и базой данных в "закрытом" контуре.

В перспективе предусматривается модернизация ПАС в части создания подсистемы визуализации с подключением к ней дополнительных функций, позволяющих:

- отображать результаты обработки на электронной карте с привязкой к географическим координатам сенсоров;
- использовать технологии GeoIP для локализации адресов атакующих машин;
- формировать отчетные документы.

В целом разработанная ПАС "Сенсор" рассматривается как средство оперативного контроля интернет-трафика в защищаемых компьютерных системах в ходе решения задачи обеспечения информационной безопасности. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ ООО "КБПМ – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"
см. стр. 52

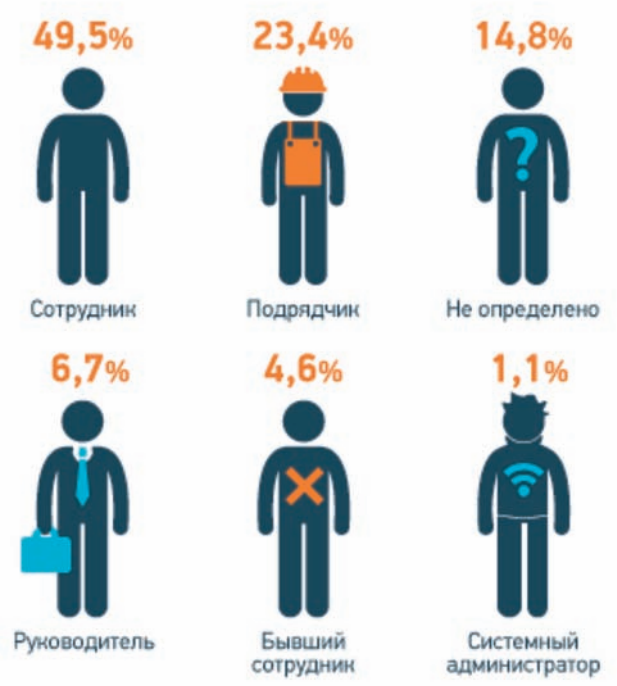
Надежный способ защиты

Олеся Бугаева, *руководитель направления по работе с заказчиками и партнерами в SMB-сегменте компании InfoWatch*

В эпоху высоких технологий информация стала дороже золота, а потому конфиденциальные данные воруют все чаще и больше. И это серьезная проблема, ведь потерявшая свои коммерческие секреты компания может попросту закрыться. Особенно если это средний или малый бизнес, существующий в высококонкурентной среде.

Но даже если этого не случится, ущерб может быть весьма серьезен: внимание и, как следствие, проверки регуляторов, переход клиентов к конкурентам, недополученная прибыль.

Иногда утечки поражают своими масштабами: например, в 2011 г. Национальная служба здравоохранения США (National Health Service) признала потерю записей о здоровье более 10 млн пациентов, связанную с флеш-накопителями и дисками с резервными копиями. Потеряны были, в том числе, и номера социального страхования, которые часто используются в различных мошеннических схемах.



В половине случаев виновниками утечек информации были сотрудники компаний – настоящие или бывшие. Согласно данным исследования аналитического центра InfoWatch.

Оперативникам УФСБ РФ по Республике Мордовия удалось пресечь деятельность преступной группы, которая занималась продажей конфиденциальной информации ООО "Торговый дом "Севкабель-Саранск" конкурентам. Им передавались сведения о ценовой политике предприятия. Обладая этими данными, конкуренты имели возможность регулировать свои цены и уводить у "Саранскkабеля" крупных клиентов. Естественно, предприятие стало нести серьезные убытки. Злоумышленники получили за эти данные 200 млн руб. Предприятие потеряло гораздо больше.

Потеря клиентов

От утечек данных страдают не только субъекты ПДн, но и компании. На персональные данные и коммерческие секреты всегда есть спрос либо со стороны мошенников, либо со стороны конкурентов. Заинтересованные лица готовы платить за нужную им информацию серьезные деньги, а для компании ценой произошедшей утечки может стать крах бизнеса.

Под ударом находится абсолютно любая компания, не уделяющая должного внимания вопросам информационной безопасности. Ведь ценность представляют ПДн, клиентские базы и финансовые сведения, а ими оперирует любая организация.

Всем известно, что сотрудники компаний часто рассматривают базу данных клиентов как свою собственность и "уносят" ее с собой, меняя место работы. Так, когда американский First State Bank открыл два новых офиса в Канзасе, он пригласил на работу лучших сотрудников конкурирующего банка – Pulaski Bank. Приглашенные сотрудники, пользуясь конфиденциальной информацией Pulaski Bank, заключали контракты с клиентами уже в интересах нового банка. Как оказалось, одна сотрудница скопировала конфиденциальную информацию на флеш-накопитель и скидывала данные, не подлежащие разглашению, с корпоративного на внешний почтовый адрес.

Иногда крадут и чисто техническую информацию: житель Набережных Челнов, некоторое время проработавший дизайнером на мебельной фабрике, получил предложение, от которого не смог отказаться. Молодой человек получил 95 тыс. руб. за то, что сбыл некоему лицу флеш-накопитель с базой чертежей и эскизов продукции фабрики, где он работал.

По данным аналитической компании Kelly Services, менее трети всех людей в мире можно назвать лояльными сотрудниками, которые стараются не допускать потери информации и соблюдать требования политики безопасности. Пример выше хорошо это подтверждает, и он далеко не единственный.

В 2011 г. Национальная служба здравоохранения США (National Health Service) признала потерю записей о здоровье более 10 млн пациентов, связанную с флеш-накопителями и дисками с резервными копиями. Потеряны были, в том числе, и номера социального страхования, которые часто используются в различных мошеннических схемах.

Главный принцип защиты

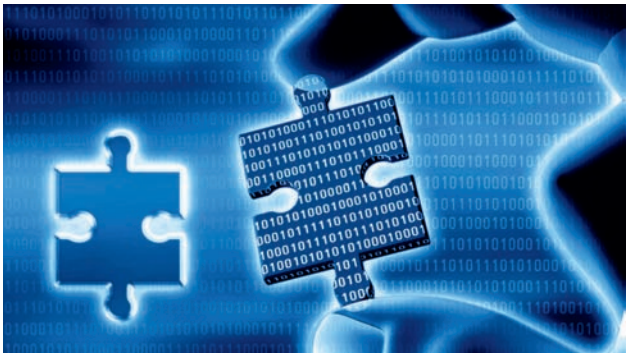
Самый надежный способ защиты от утечек через съемные носители – это шифрование. Найти инструменты, реализующие шифрование, нетрудно. Гораздо сложнее выбрать среди них наиболее эффективный. Главный принцип защиты информации заключается в том, что затраты на нее не должны превышать ущерба, который может нанести потеря или кража этой информации.

Поэтому для защиты данных на съемных носителях оптимально использовать систему, которая, как минимум, не потребует сложного внедрения и штата специалистов для поддержки, а в идеале будет обладать более широкой функциональностью, чем просто шифрование данных на флеш-накопителях.

Современная система шифрования должна защищать данные не только на съемных носителях (включая, но не ограничиваясь флешками), но и в облачных хранилищах, файлы и папки на локальных и сетевых ресурсах.

Удобнее, если шифрование будет осуществляться в прозрачном режиме, то есть незаметно для пользователей. При этом администратор системы должен иметь возможность указать типы данных и сценарии, для которых информация будет шифроваться принудительно либо по инициативе пользователя.

Чем более гибкое и многоуровневое разделение прав доступа к зашифрованной информации предоставляет система, тем она эффективнее и удобнее в использовании. Администратор должен иметь возможность настраивать самые различные правила, начиная с отдельного сотрудника или отдела и заканчивая всей компанией. Ну и, конечно, необходимо иметь возможность расшифровывать файлы на сторонних компьютерах с помощью пароля.



Если система защиты корпоративных данных удовлетворяет перечисленным выше требованиям, то перед вами действительно надежный инструмент, который сможет защитить ваш бизнес от утечек информации. ●

Самый надежный способ защиты от утечек через съемные носители – это шифрование. Найти инструменты, реализующие шифрование, нетрудно. Гораздо сложнее выбрать среди них наиболее эффективный. Главный принцип защиты информации заключается в том, что затраты на нее не должны превышать ущерба, который может нанести потеря или кража этой информации.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

О действенных методах защиты съемных носителей

Светлана Конявская, *заместитель генерального директора "ОКБ САПР"*

Что может предпринять злоумышленник в отношении флешки как носителя информации, включенного в интересующую его информационную систему? Есть всего несколько типов распространенных атак на флешки:

1. Кража или находка.
2. Отъем.
3. Завладение оставленным без присмотра устройством.
4. Завладение путем мошенничества и социальной инженерии.
5. Покупка у мотивированного инсайдера.

Как правило, пп. 1, 2 и 5 имеют своей целью завладение данными с флешки, а пп. 3 и 4 могут также иметь целью внедрение подложных данных или вредоносного кода (реже, но тоже возможно – уничтожение данных на флешке).

Очевидно, что защитить маленькое устройство от физической кражи (или находки в результате целенаправленного поиска в местах возможных потерь, провокации потери) – крайне сложно.

Значит, задача защиты флешки сводится к тому, чтобы сделать нелегальное физическое обладание ею бессмысленным. То есть, даже имея флешку, получить доступ к данным на ней где-то, кроме разрешенного явно компьютера, кому-то, кроме разрешенного явно пользователя, должно быть невозможно.

Именно эта логика и положена в основу защищенных флешек семейства "СЕКРЕТ". Управляющий элемент в СН "Секрет" "коммутирует" компьютер с диском "Секрета" (собственно флешкой) только после успешного завершения контрольных процедур – взаимной аутентификации СН, компьютера и пользователя.

Дополнительно защитные свойства "Секрета" могут быть усилены шифрованием данных при записи на диск. Выбирать такой носитель целесообразно тогда, когда разумно предположение, что злоумышленник может попытаться считать данные с флеш-памяти напрямую, например, выпаяв ее с устройства.

Сравним эффективность противодействия перечисленным выше атакам традиционными способами и с применением "Секретов".

Находка или кража

Потеряв флешку, невозможно быть уверенным ни в том, потеряна она или украдена, ни в том, что случайно нашедший ее человек не воспользуется записанными данными.

В этой ситуации совершенно не успокаивает наличие в системе USB-фильтров. Это утешение звучит даже несколько издевательски.

Насколько в этой ситуации может успокоить **PIN-код** – вопрос философский. Примерно настолько же, насколько успокоительна мысль о том, что никто не станет поднимать валяющуюся флешку. Хорошо, если так, а если нет, то PIN-код подберут, и очень легко. Предназначенные для этого программы сегодня есть у каждого студента. Теоретически можно бороться с этим, увеличивая длину PIN-кода. Но чем длиннее PIN-код, тем выше вероятность того, что он записан на корпусе флешки.

Биометрия

Отпечаток пальца "подобрать" сложнее, чем PIN-код. Но если задуматься о том, как может быть реализована биометрическая аутентификация в обычной флешке, то становится ясно, что эталон хранится на самой же флешке, а сравнение производится в оперативной памяти ПК (так как у флешки нет своих вычислительных ресурсов). Все следствия очевидны:

- у системы есть доступ к флешке до аутентификации (иначе как она получит эталон?);
- решение "сошлось" принимается в оперативной памяти компьютера.

Это значит, что на специально подготовленном компьютере (иными словами, на своем) злоумышленник сможет открыть флешку.

Шифрование данных на флешке

Пожалуй, самый убедительный из традиционных способов. Однако ограничения у этого способа все те же, что описаны выше в отношении биометрии.

Где-то на флешке хранится ключ, на котором в оперативной памяти ПК будут расшифровываться данные. Чтобы система получила доступ к ключу, нужно корректно аутентифицироваться. Таким образом, шифрование вообще никак не повышает защищенность флешки с PIN-кодом или "пальцем", так как задача сводится к предыдущему случаю – передать данные о корректной аутентификации.

Как же обстоит дело в случае применения "Секрета"?

Злоумышленник добыл "Секрет" и подключает его к своему "специально обученному" компьютеру.

Все, что он увидит, – некое "другое устройство" в "Устройствах". Ни одного "съемного диска" в "Моем компьютере" не появится, запроса PIN-кода тоже.

Доступа к диску "Секрета" и к данным, которые его открывают, нет ни у пользователя, ни у системы, поэтому запускать какие-то свои специальные программы злоумышленнику бессмысленно.

Отъем

Надо отдавать себе отчет в том, что злоумышленник понимает: за такую мелочь, как флешка, скорее всего, человек не будет биться до последнего, и в общем случае сработает вариант отобрать и, оказав психологическое давление (а сам факт отъема окажет на большинство людей известное психологическое давление!), выяснить **PIN-код**, если он имеется.

Фантазировать насчет **биометрии** – совершенно не хочется.

Шифрование не поможет по тем же причинам: выяснить данные, необходимые для доступа к ключу, несложно.

Как же обстоит дело в случае применения "Секрета"?

Смело отдавайте флешку и называйте PIN-код, не подвергайтесь опасности физического воздействия. Пускай злоумышленник уносит все это: на его компьютере "Секрет" не примонтируется и не запросит PIN-код.

Развивая сюжет боевика, можно вообразить ситуацию, что злоумышленник взял владельца с собой, чтобы убедиться, что тот назвал ему верный PIN-код. Мол, если не подойдет – поговорим по-другому.

Ничего страшного, он сам убедится, что "флешка сломанная" – не появляется диск в "Моем компьютере", и все тут.

Завладение оставленным без присмотра устройством

Наверное, самый распространенный способ получить чужую флешку – это взять там, где пользователь ее бросил "на 5 минут", вздремнув или отойдя попить кофе.

С точки зрения противодействия злоумышленнику этот случай не отличается от случая с кражей. С точки зрения действий злоумышленника по обходу этих защитных мер и получению доступа к диску флешки – тоже.

Однако есть существенная деталь, заставляющая рассматривать эту ситуацию как отдельную. В случае с кражей или потерей владелец устройства знает о том, что инцидент произошел. В описываемой же ситуации вполне реально представить все так, будто ничего и не было. Пользователь видит флешку на месте и не имеет ни малейших оснований для опасений, что его данные стали кому-то известны, а возможно, искажены, а возможно, флешка заражена вирусами или иными вредоносными программами.

И если для подбора PIN-кода или иной аутентифицирующей информации для доступа к данным (или к ключу для расшифрования данных) компьютер (ноутбук) злоумышленника должен быть снабжен минимальным инструментарием, а сам злоумышленник должен иметь минимальную квалификацию, то для того, чтобы записать на флешку вредоносный код или просто заразить ее вирусами, ничего этого не нужно.

Как уже упоминалось выше, любая флешка с аутентификационными механизмами должна "пускать" к себе систему ПК, так как верификация предъявленных аутентифицирующих данных должна производиться в оперативной памяти компьютера, в которую необходимо загрузить эталон, хранящийся на флешке (система должна получить доступ к флешке, чтобы получить данные для проведения аутентификации).

У системы есть доступ к флешке, значит, есть он и у вредоносного ПО. Game over.

Как же обстоит дело в случае применения "Секрета"?

До успешного прохождения взаимной аутентификации "Секрета" с компьютером и успешной аутентификации пользователя в устройстве взаимодействие производится только с модулем аутентификации "Секрета", который физически отделен от флеш-памяти. Флеш-диск при этом не примонтирован и недоступен системе – ни на чтение, ни на запись.

Злоумышленник может экспериментировать с устройством сколько угодно, но на диск устройства при этом ничего не запишется, пока злоумышленник не пройдет все этапы аутентификации.

Ну а тот факт, что и пройти все этапы аутентификации ему не удастся, был уже доказан выше.

Заметим, что для случаев, когда важно не только не допустить успешной реализации такой атаки, но и знать обо всех попытках атак, в продукте "Секрет Особого Назначения" ведется аппаратный журнал событий, в котором фиксируются все без исключения попытки подключения устройства к различным компьютерам – вне зависимости от того, успешной или нет была попытка.

Если у вас возникли хоть малейшие подозрения (флешка, кажется, лежала не совсем здесь) – их можно проверить, чтобы знать точно.

Завладение путем мошенничества и социальной инженерии

По сути дела, это "мягкий" вариант "отъема", отягченный, впрочем, дополнительными обстоятельствами:

- пострадавший не знает (во всяком случае, в первый момент), что стал жертвой покушения, – и не предпринимает своевременных мер;
- при определенной квалификации мошенник может выстроить многоступенчатый сценарий атаки на систему, включающий не только единовременное завладение флешкой, но также и подмену данных, то же заражение системы или внедрение в нее нужных ему закладок.

Очевидно, что если флешки с **PIN-кодом**, **биометрией** и **шифрованием** бессильны в случае отъема и кражи, бессильны они и в этом случае. Наоборот, доверяя злоумышленнику, пользователь не только введет PIN-код и приложит палец, но и проследит, чтобы у злоумышленника все было хорошо.

Как же обстоит дело в случае применения "Секрета"?

Возможны два сценария развития событий в зависимости от того, как построена система работы с "Секретами" в организации.

Если пользователь не знает, как организована система защиты, а работает просто по факту – "на легальных компьютерах работать сможешь, на нелегальных – нет", он подумает, что либо компьютер нелегальный (и заподозрит злоумышленника), либо флешка сломалась. Так или иначе, даже будучи предельно доверчивым, помочь злоумышленнику открыть "Секрет" он не сможет.

Если же пользователь в курсе, как работает "Секрет", то он будет уверен: человек, который его склоняет отдать флешку, либо будет ее использовать в рамках легальной системы, а значит, "свой", либо не сможет использовать "Секрет".

Покупка у мотивированного инсайдера

Совершенно невозможно спорить с тем, что ни **PIN-код**, ни **биометрическая** аутентификация, ни **зашифрование/расшифрование** данных на флешке на основании введенных аутентификационных данных пользователя не могут защитить от того, что легальный пользователь сам может отдать флешку заинтересованным лицам на привлекательных для себя условиях, или скопирует данные на домашний компьютер и отправит куда-то по почте, или принесет в информационную систему какие-то программы или данные в интересах третьих лиц.

Легальный пользователь – полновластный хозяин флешки.

Неужели с этим нужно смириться и подозревать всех, кто работает с флешками, каждый раз, когда они унесли их домой? Ведь проверить, "было или не было", невозможно.

Как же обстоит дело в случае применения "Секрета"?

Основной этап системы контроля доступа в "Секрете" – взаимная аутентификация "Секрета" и компьютера. В "Секрете" есть база компьютеров, а на компьютерах – база "Секретов". Только после того, как "Секрет" опознал компьютер, который для него разрешен, а компьютер опознал "Секрет", которому можно на нем работать, процедура контроля доступа переходит к стадии аутентификации пользователя.

Будь пользователь абсолютно легальным – "Секрет" даже и не узнает об этом, если подключить он (пользователь) его ("Секрет") пытается к "постороннему" компьютеру.

В таком случае просто бессмысленно уносить "Секрет" с собой.

Если же владелец хочет не только иметь уверенность в том, что флешка не была использована на чужих компьютерах, но и иметь возможность в любой момент проверить честность своих сотрудников – проверить, не пытались ли они сделать что-то подобное, – то этого можно добиться, используя "Секрет Особого Назначения". В "Секрете Особого Назначения" в специальном аппаратном журнале администратор может увидеть записи обо всех случаях подключений, даже неудачных. Это даст возможность не сомневаться, а проверить – и убедиться в добросовестности своих сотрудников. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ ЗАО "ОКБ САПР"
см. стр. 52

Темная сторона криптографии

Угроза клептографии обсуждается с середины 1990-х гг., но существенное внимание она привлекла лишь недавно. Этому есть два объяснения: во-первых, в Интернете все чаще обсуждается именно этот вид высокотехнологичной атаки, а во-вторых – увеличилось число задокументированных клептографических атак.

При изучении задокументированных особенностей подобного рода атак мы видим, что одной из основных специфик взлома методом клептографии служит выяснение механизма шифрования, использующегося на компьютере жертвы. Защитные аппаратные модули, смарт-карты и Trusted Platform Modules (TPMs) широко применяются для защиты от всех воздействий извне. Но в то же время эти устройства вызывают у своих владельцев определенные вопросы: "Как пользователь может убедиться, что "черный ящик" такого устройства выполняет только то, для чего он официально был выпущен, и не делает ничего другого?".

Нельзя с уверенностью сказать, взаимодействует ли криптосистема таких устройств с содержимым компьютера пользователя, и можно ли снять подозрения с потока информации, генерируемого устройством с компьютера вовне. Но, так или иначе, пользователю приходится безоговорочно довериться фирме-изготовителю защищенного аппаратного модуля и любого другого подобного устройства и верить, что с его данными устройство никак не взаимодействует.

Как удостовериться в том, что все те схемы и описания, которые предоставляет фирма-изготовитель, соответствуют устройству, которое в итоге попадает к пользователю в руки? Более того, не нужно быть специалистом в области конспиративных теорий, чтобы осознать, какое влияние могут оказывать государственные организации на изготовителей. Так как же можно удостовериться в том, что на самом деле происходит внутри устройств, которыми мы пользуемся, устройств – черных ящиков?

Клептография

Клептография – это изучение науки о незаметном для пользователя похищении информации. Клептографические атаки – это хакерские атаки, в ходе которых злоумышленник использует асимметрическую систему криптографии для осуществления взлома в форме криптографического бэкдора*. В этом случае криптография применяется против криптографии: бэкдор не является еще одним каналом связи с внешним миром за пределами криптосистемы, и для такой кражи нет нужды передавать дополнительную информацию. Бэкдор здесь используется вместо хакерской программы, требующей встраивания в программу, данные которой необходимо похитить. Таким образом, клептография – один из объектов изучения криптовирусологии, науки о применении криптографии во вредоносных программах. Целью клептографических атак являются не детали общего вида ПО компьютера, а детали специфической среды системы шифрования.

Следующий пример описывает возможную клептографическую атаку. "Черный ящик" внутри подсоединяемого к компьютеру устройства генерирует асимметрические пары ключей, один из которых – закрытый, а другой – открытый. Закрытый ключ, который используется в расшифровке и генерации цифровой подписи, должен оставаться исключительно внутри "черного ящика", чтобы предотвратить ненадлежащее использование и дублирование; открытый ключ может быть свободно распространен. Принято считать, что никто не может получить закрытый ключ, преобразовав открытый, но так ли это на самом деле?

А вот и лазейка

На самом деле такая возможность есть, если сам процесс генерации ключей был изменен определенным образом. Бэкдор может быть встроен в процессе изготовления криптосистемы таким образом, чтобы предоставить злоумышленнику доступ к закрытому ключу, не привлекая к нему внимания. Это будет незаметно, потому что сгенерированные открытые ключи появятся без всплывания окошек и прочих информационных системных сообщений. Получив копию секретного ключа, злоумышленник получает особые возможности: подделать подписи и получить доступ к расшифровкам секретных данных. Он получает эти возможности, хотя несанкционированный доступ к содержимому "черного ящика" не был разрешен в принципе.

Манипуляции такого рода могут быть раскрыты "реверсивной инженерией", если исследователей не остановит механизм безопасности черного ящика. Так как генератор псевдослучайного числа закреплен в исходном коде, с помощью реверсивной инженерии можно вычислить секретный код вне "черного ящика". С точки зрения хакера, крайне желательно иметь эксклюзивный доступ к механизму атаки, чтобы затруднить расследование. А в случае усиления защиты со стороны хакеров реверсивную инженерию и вовсе можно исключить из способов борьбы с такого рода угрозами. ●

По материалам: www.infosecurity-magazine.com

Упрощенно объяснить, как устроена клептографическая хакерская атака, можно следующим образом. Речь идет о манипуляции генератором случайных чисел внутри шифровальной схемы. В случае взлома процесс генерации случайного числа изменится, и будет выбрано псевдослучайное число вместо действительно случайной числовой последовательности. Зная основные цифры, сгенерированные криптосистемой, хакеру не составит труда сгенерировать закрытый ключ вне "черного ящика" устройства.

* back door – взлом в фоновом режиме, в ходе которого важная информация с компьютера передается злоумышленнику незаметно.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Биометрическая идентификация нового поколения от "Аладдин Р.Д." – концепция Match-on-JaCarta

Антон Крячков, *руководитель направления управления знаниями, компания "Аладдин Р.Д."*

В статье, опубликованной в "Information Security" № 6 (2013), мы начали обсуждать преимущества и особенности использования криптографических и биометрических средств для обеспечения информационной безопасности. В продолжение этой темы в текущей статье речь пойдёт о новых перспективных разработках компании "Аладдин Р.Д." в области биометрической идентификации.

Компания "Аладдин Р.Д." предлагает технологию JaCarta BIO, которая вобрала в себя все лучшее, что присуще современной биометрии. Процесс аутентификации прост, быстр и интуитивно понятен. Решение максимально комфортно для пользователя, вероятность ошибок минимальна, а время, необходимое для сканирования отпечатка, не превышает секунды.

В основе нашей технологии лежит архитектура Match-on-Card (сравнение на карте).

К настоящему времени компания "Аладдин Р.Д." завершила разработку нового поколения аппаратных комбинированных считывателей отпечатков пальцев и смарт-карт, работающих со смарт-картами основе архитектуры Match-on-Card, и обеспечивающих повышенную защищенность при использовании смарт-карт в недоверенной среде.

Существуют различные концепции биометрических систем доступа по отпечаткам пальцев. Системы отличаются местом, где эталонные шаблоны хранятся, сравниваются с контрольными шаблонами и где принимаются решения об их идентичности:

- Match-on-Server – сравнение шаблонов происходит на сервере биометрической аутентификации. В данной схеме эталонные шаблоны хранятся в зашифрованном виде в централизованной базе данных, а контрольный шаблон для сравнения пересылается центральному серверу. Сервер биометрической аутентификации принимает решения о совпадении шаблонов и выдает разрешения на дальнейшие действия.
- Match-on-PC – хранение, сравнение шаблонов и принятие решения о совпадении происходит на рабочей станции пользователя. Очень распространённая и доступная схема. Сканер отпечатка пальцев может быть встроен в персональный компьютер (ноутбук) пользователя.
- Match-on-Card – эталонные шаблоны пользователя хранятся в защищенной памяти его персональной смарт-карты. Все необходимые вычисления для сравнения шаблонов также выполняются "на борту" смарт-карты.
- Match-on-Device – хранение, сравнение шаблонов и принятие решения о совпадении происходит на сканере отпечатков пальцев. Преимуществом такого подхода является то, что аутентификационно опасная информация (рисунок отпечатка пальца, готовый шаблон) проходит полный цикл обработки непосредственно на сканере и не передается на рабочую станцию пользователя.

Match-on-Card + Match-on-Device = Match-on-JaCarta

В настоящее время наиболее перспективным решением является объединение технологий и наработок, реализованных в рамках существующих концепций Match-on-Card и Match-on-Device.

В рамках концепции Match-on-JaCarta компания "Аладдин Р.Д." предлагает:

- весь цикл обработки рисунка отпечатка пальца и шаблона (получение рисунка, формирование шаблона, передача шаблона на смарт-карту для записи/сравнения) выполнять непосредственно в самом комбинированном считывателе отпечатков пальцев и смарт-карт;
- сравнение эталонного и контрольного шаблонов выполнять на смарт-карте.

Результатом выполнения операции биометрической аутентификации является, как и ранее, предоставление или отказ в предоставлении доступа к смарт-карте в режиме пользователя.

Сохраняются все преимущества технологии Match-on-Card, а именно:

- безопасное хранение эталонных шаблонов в памяти смарт-карты;
- сравнение эталонных шаблонов с контрольными шаблонами происходит в смарт-карте;
- невозможность экспорта эталонных шаблонов из памяти смарт-карты (две последних возможности обеспечиваются операционной системой смарт-карты).

Добавляются преимущества технологии Match-on-Device, а именно:

- исключаются передача обработка аутентификационно опасной информации (рисунок отпечатка пальца, шаблон) на рабочей станции пользователя, которая, как правило, является недоверенной средой и может содержать вредоносное ПО;
- вся работа с аутентификационно опасной информацией осуществляется в системном ПО (firmware) комбинированного считывателя.

Исключаются недостатки технологии Match-on-Device, а именно:

- местом хранения эталонных шаблонов (шаблона) по-прежнему является смарт-карта пользователя, сам же считыватель не хранит никаких шаблонов и является универсальным, легко заменяемым и непривязанным к конкретному рабочему месту и/или пользователю.

В настоящее время компания "Аладдин Р.Д." завершила разработку универсального считывателя для отпечатков пальцев и смарт-карт, согласно концепции Match-on-JaCarta. В ближайшее время все заинтересованные лица смогут присоединиться к программе тестирования созданного компанией решения.

Важным преимуществом Match-on-Card является то, что хранение цифровых образцов отпечатков и принятие решения свой/чужой выполняются в защищённой области смарт-карты, а не на сервере биометрической идентификации. Цифровые образы отпечатков никуда не пересылаются. Не создаются биометрические базы данных пользователей. Таким образом, даже администраторы системы не имеют доступа к биометрической информации сотрудников.

В основе технологии JaCarta BIO лежит концепция Match-on-Card. Смарт-карта, являясь важнейшим компонентом PKI-инфраструктуры, хранит в памяти пароли, закрытые ключи, сертификаты доступ к которым открывается только после проверки биометрических данных. Эталонные шаблоны отпечатков хранятся в защищенной памяти смарт-карты. Все необходимые вычисления для сравнения шаблонов также выполняются "на борту" смарт-карты. По результатам сравнения предъявленного (контрольного) и хранящегося (эталонного) шаблонов смарт-карта принимает решение о предоставлении или отказе в предоставлении доступа пользователя к данным смарт-карты.

NM
АДРЕСА И ТЕЛЕФОНЫ компании "АЛАДДИН Р.Д. см. стр. 52

Что первично: требования бизнеса или требования регуляторов?

Дмитрий Дудко, *руководитель проектов по информационной безопасности центра компетенции ИБ, ЗАО "Фирма АйТи. Информационные технологии"*

Удивительно, что вопрос, поставленный в заголовке статьи, до сих пор вызывает споры. Ведь в том случае, если бизнес готов полностью подстраиваться под требования регуляторов, данный вопрос уходит с повестки. А во всех остальных реальных случаях первичны требования бизнеса. Почти у каждой организации есть сформулированная миссия, цель ее работы — иногда это большой документ, лозунг или неформальная идея. Но она есть всегда.

Разумеется, у коммерческих организаций на первом месте получение прибыли. Всегда интересно, что идет за этим. И я уверен, что не найдется бизнеса в нашей стране, у которого дополнительной миссией будет нарушение законов РФ. Однако иногда требования регуляторов идут в разрез с основной идеей бизнеса. Давайте разберем причины их противоборства.

Я ни в коем случае не призываю безопасников нарушать закон. Как мы уже выяснили, регулятор не имеет желания разрушить ваш бизнес, обанкротив его своими требованиями. Регулятор защищает бизнес от лишних затрат, связанных с реализованными угрозами безопасности, однако он не может учитывать всех особенностей самого бизнеса. Нам, безопасникам, остается лишь искать законные решения, которые позволят организациям оставаться на плаву.

Для начала я хотел бы рассказать одну историю

Когда-то я занимался проектом по защите ПДн в одной обучающей организации с крайне сложной базой этих самых данных, раскиданной по всему СНГ, с запутанными связями. Как уже стало понятно из вышесказанного, имела место трансграничная передача данных. Однако данные эти лишь с натяжкой можно было назвать персональными. Передача производилась по незащищенному каналу, и за много лет существования организации ни один человек не пострадал. Однако регулятор требовал защиты канала передачи по полной и очень дорогой программе. Заказчик и моя команда понимали, что такое решение организации просто не потянуть. Пришлось искать пути законного обхода требований. С большим трудом они были найдены, организация осталась жива. Так что это получается? Регулятор уничтожает бизнес?

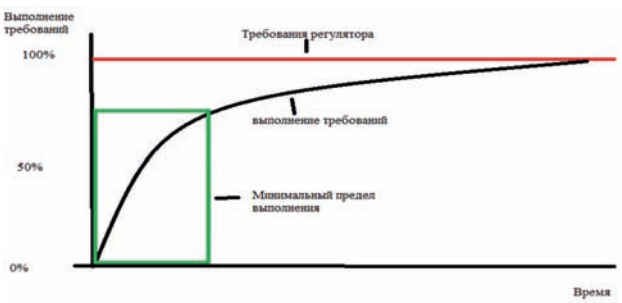


Рисунок. Зависимость выполнения требований от времени

Разумеется, это не так

Регулятор – это не злейший враг из приключенческого романа, который призван строить различные козни бравым героям. В первую очередь, регулятор помогает разобраться в законах, установить единые правила игры для всех. И в этом-то и кроется главный камень преткновения. По своему опыту разработки отраслевых стандартов для медицины и учебных заведений могу сказать, что задача унификации требований или рекомендаций крайне сложна. Каким бы набором исходных данных вы ни обладали, как бы хорошо ни провели типизацию объектов, всегда ваши требования будут менее конкретизированными и не будут подходить на 100% какой-либо организации. И это лишь в рамках одной отрасли. Увеличьте это в масштабах страны и умножьте неопределенность на количество отраслей.

Таким образом, задача регулятора – добиться единообразия для совершенно разных отраслей и организаций. Требования приобретают более общий характер, и именно здесь кроются все возможные возникающие противоречия. Например, если требования по сбору согласий на обработку ПДн могут выполнить большинство обычных юридических лиц, то интернет-магазину это будет крайне затруднительно.

Но совершенно точно можно сказать, что минимум ¾ требований может выполнить подавляющее большинство.

Зависимость выполнения требований от времени

На рисунке представлена аналитическая зависимость выполнения требований от времени. В данном случае минимальным пределом выполнения требований является та общность, что присуща любой компании, подпадающей под регулирование. На оставшуюся часть приходятся индивидуальные особенности.

Аналогичная зависимость подходит для любого другого ресурса, который мы используем для реализации требований (чаще всего это деньги и время).

Совершенно логично, что как только речь заходит о капиталовложениях, решение остается за бизнесом.

Таким образом, логичный ответ на вопрос в заголовке – первичны требования бизнеса. Всегда.

Помните, вы – доверенное лицо. Вы обязаны защищать организацию, на которую работаете, минимизировать риски, сделать максимум доступными средствами и бороться за свою компанию при проверке до последней капли крови. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Рецепты по управлению рисками ИБ

Алена Килина, *CISA, эксперт практики аудит и консалтинг ИБ "Астерос Информационная безопасность"*

Любая компания ставит перед собой бизнес-цели и осуществляет в соответствии с ними свою деятельность. При этом всегда существует вероятность возникновения тех или иных событий, которые могут негативным образом повлиять на достижение поставленных целей. Управление рисками, в том числе и в сфере информационной безопасности, помогает определить области, наиболее подверженные угрозам, и принять обоснованное решение относительно стратегии их обработки.

Дьявол кроется в деталях

На сегодняшний день существует множество подходов и методик оценки рисков ИБ. Однако на практике специалисты сталкиваются с рядом вопросов. Выражение "Дьявол кроется в деталях" здесь как никогда актуально. Рассмотрим наиболее распространенные заблуждения и ошибки, которые возникают в процессе управления рисками ИБ.

Процесс управления рисками ИБ не интегрирован с процессами управления рисками компании в целом

Хорошей практикой является, если риски ИБ оцениваются и обрабатываются в рамках общего процесса управления рисками компании (Enterprise Risk Management, ERM), тесно связанного с целями бизнеса. Это позволяет учитывать их влияние на достижение бизнес-целей компании.

Отсутствует роль "владелец риска"

В новой редакции международного стандарта ISO/IEC 27001–2013 введено понятие "владелец риска", означающее, что для контроля за каждым рисковым событием назначается ответственное лицо. В идеале это должны быть топ-менеджеры, поскольку они обладают соответствующими полномочиями и необходимыми ресурсами (например, финансовыми или трудовыми) для принятия решений. Однако на практике чаще на эту роль назначаются сотрудники подразделений ИБ и/или IT. В таком случае рекомендуется рассматривать риски ИБ с точки зрения их влияния на ключевые для бизнеса процессы. Это позволит обосновать перед руководством компании выделение бюджета на их обработку.

"Твоя моя не понимай": представление результатов оценки рисков ИБ руководству в терминах IT и ИБ

Руководство компании оперирует "терминами бизнеса", и зачастую ему неочевидно, к примеру, влияние работоспособности конкретного сервера или приложения на достижение бизнес-целей компании. Следовательно, в процессе оценки рисков, на этапе идентификации активов необходимо проанализировать бизнес-процессы, выявить и показать связь с активами, обеспечивающими их выполнение (до этого в компании должны быть определены и описаны основные процессы ее деятельности).

Результаты реализации мер по снижению рисков ИБ также необходимо предоставлять руководству в привычных для него терминах, например в виде соотношения затрат на реализацию мер ИБ и предотвращенных потерь от негативных событий (Return on Investment for Security, ROSI). Данная величина рассчитывается в денежных единицах и характеризует результат инвестирования в ИБ.

Использование сложных математических методов для оценки ущерба с целью демонстрации их значимости

Например, в стандарте ГОСТ Р ИСО/МЭК 31010–2011 или ISO/IEC 31010–2009 описан 31 метод оценки рисков, большая часть из которых сложно реализуема с практической точки зрения. Критерием выбора метода оценки ущерба и вероятности его возникновения должна быть возможность применения метода на практике, а не научность и математическая сложность.

Снижение рисков до "нулевого" уровня

Как бы ни хотелось, но снизить риски до "нуля" просто невозможно. Даже после реализации комплекса мер по их снижению всегда будут присутствовать "остаточные" риски. Основной вопрос – являются ли они приемлемыми для компании. В данном случае в компании должен быть установлен уровень приемлемого риска (риск-аппетит) и решение о способе обработки должно приниматься руководством.

Риски оцениваются один раз

Оценку необходимо проводить на регулярной основе, поскольку, во-первых, компания осуществляет свою деятельность в постоянно изменяющейся среде – запуск новых услуг, внедрение новых систем, применение новых технологий и прочее. Это сопровождается возникновением соответствующих угроз. Во-вторых, после проведения первичной оценки и реализации комплекса мер необходимо отслеживать динамику уровня рисков.

Также рекомендуется вести "Карту рисков", позволяющую видеть данные изменения. Она может использоваться для представления результатов оценки и обработки рисков руководству компании.

В заключение

После разбора наиболее распространенных ошибок и заблуждений рассмотрим вопросы автоматизации процесса управления рисками ИБ: как оценить ее целесообразность, с чего начать и какие "подводные камни" подстерегают на этом пути. Данный вопрос заслуживает отдельного внимания. ●

Продолжение следует...

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Хорошей практикой является, если риски ИБ оцениваются и обрабатываются в рамках общего процесса управления рисками компании (Enterprise Risk Management, ERM), тесно связанного с целями бизнеса. Это позволяет учитывать их влияние на достижение бизнес-целей компании.

Смарт-карт ридер для iPhone/iPad/iPod с разъемом Lightning

Производитель: ЗАО "Аладдин Р.Д."
Сертификат:
- изделие не подлежит сертификации
- MFi, RoHS, CE, FCC, EMV Level 1

Назначение:
- обеспечивает использование усиленной квалифицированной ЭП
- для использования в мобильных приложениях, требующих применения сертифицированных российских СКЗИ, двухфакторной аутентификации пользователей, хранения ключевых контейнеров на смарт-картах

Особенности:
- подключается через стандартный разъем Lightning ко всем моделям iPhone/iPad/iPod
- подключается с помощью кабеля через разъем USB к персональным компьютерам

Возможности:
- работа со смарт-картами, соответствующими требованиям ISO7816
- возможность работы с эмбоссированными картами

Характеристики:
- дизайн корпуса соответствует дизайну устройств iPhone/iPad/iPod
- надежность: в изделии используются алюминиевые корпусные элементы
- контактная группа обеспечивает срок службы карт без механических повреждений не менее 3 лет
- световой индикатор режима работы
- малые габариты и масса
- соответствует стандартам: PC/SC, CCID, ISO7816, EMV, USB 2.0

Ориентировочная цена: 2190 руб. (рекомендованная розничная цена)
Время появления на российском рынке: декабрь 2013 г.
Фирма, предоставившая информацию: АЛАДДИН Р.Д.

См. стр. 47

Беспроводной смарт-карт ридер для мобильных устройств

Производитель: ЗАО "Аладдин Р.Д."
Сертификат: изделие не подлежит сертификации
Назначение:
- обеспечивает использование усиленной квалифицированной ЭП на различных мобильных устройствах
- предназначен для считывания информации со смарт-карт и записи на них необходимых данных
- позиционируется для использования с различными мобильными устройствами на различных платформах благодаря встроенному в решение модулю соединения по технологии Bluetooth

Особенности: работает от встроенного аккумулятора по протоколу Bluetooth 4.0 с шифрованием канала связи по AES
Возможности:
- подключение по microUSB к ПК и ноутбукам с помощью входящего в комплект кабеля
- работа с любыми процессорными смарт-картами, удовлетворяющими требованиям ISO7816

Характеристики:
- размеры – 64x86x12 мм
- масса – 56/38 г (с батареей/без батареи)
- емкость аккумулятора – 890 мАч (10–11 ч непрерывной работы или 100 ч в режиме ожидания)
- соответствует требованиям стандартов IEC 60529 (DIN 40050, ГОСТ 14254–96), обеспечиваемая степень защиты – IP68
- соответствует стандартам: CCID, ISO7816, EMV, USB 2.0, IEEE 802.11

Ориентировочная цена: 3490 руб. (рекомендованная розничная цена)
Время появления на российском рынке: декабрь 2013 г.
Фирма, предоставившая информацию: АЛАДДИН Р.Д.

См. стр. 47

Пластиковый чехол для iPad mini со встроенным смарт-карт ридером

Производитель: ЗАО "Аладдин Р.Д."
Сертификат:
- изделие не подлежит сертификации
- соответствует требованиям MFi, RoHS, CE, FCC, EMV Level 1

Назначение:
- обеспечивает использование усиленной квалифицированной ЭП на всех Apple iPad mini
- для удобного использования с мобильными устройствами iPad mini и iPad mini 2 в приложениях, где требуется применение сертифицированных российских СКЗИ, технологий смарт-карт, двухфакторной аутентификации пользователей, хранение ключевых контейнеров на отчуждаемых носителях

Особенности:
- для подзарядки не требуется снимать чехол
- в комплект поставки входит кабель USB – microUSB
- совместим со Smart Cover для iPad mini

Возможности:
- работа со смарт-картами, соответствующими требованиям ISO7816
- возможность работы с эмбоссированными картами

Характеристики:
- контактная группа обеспечивает срок службы карт без заметных механических повреждений не менее 3 лет
- световой индикатор режима работы
- соответствует стандартам: ISO7816, EMV, USB 2.0

Ориентировочная цена: 3890 руб. (рекомендованная розничная цена)
Время появления на российском рынке: декабрь 2013 г.
Фирма, предоставившая информацию: АЛАДДИН Р.Д.

См. стр. 47

Программно-аппаратная система "Сенсор"

Производитель: ООО "КБПМ – информационная безопасность"
Сертификат: изделие подлежит сертификации
Назначение: выявление вредоносного ПО и сетевых атак в режиме реального времени трафика на скорости 1 Гбит/с
Особенности: систематизация выявленной информации, формирование статистических характеристик
Возможности: проведение экспресс-анализа накопленных данных; технический мониторинг
Характеристики: протоколы выявления вредоносного ПО: HTTP, SMTP, POP3, FTP, СУБД PostgreSQL
Ориентировочная цена: 1 млн руб.
Время появления на российском рынке: готовится к выходу
Подробная информация: http://kbpm-ib.ru/paskapvo
Фирма, предоставившая информацию: КБПМ – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ООО

См. стр. 40, 41

Программно-аппаратный комплекс "Пункт-МС"

Производитель: ООО "КБПМ – информационная безопасность"
Сертификат: положительное заключение о соответствии образца комплекса требованиям "Задания по безопасности" и о возможности использовать его для проведения проверок сменных носителей на наличие компьютерных вирусов, выдано ФСБ РФ
Назначение: проверка сменных носителей информации (СНИ) на наличие компьютерных вирусов (КВ), причем СНИ могут содержать информацию как открытую, так и содержащую сведения, составляющую государственную тайну
Особенности:
- сигнатурный способ обнаружения вирусов
- типы проверяемых СНИ: CD-R, CD-RW, DVD+R, DVD+RW, IDE HDD, SATA HDD, флеш-карты (CF, MMS, MS, CD), флеш-карты для порта USB

- типы файловых систем: FAT, FAT16, FAT32, NFTS, EXT2, EXT3, ISO 9660
- вывод отчета о проверке на бумажный носитель
- возможность доработки моделей по требованиям заказчика

Возможности:
- обеспечена возможность регулярно обновлять базы сигнатур с флеш-карты
- проверка носителя информации, распечатка результатов, выключение комплекса происходят автоматически, без участия оператора

Ориентировочная цена: 135 000 руб.
Время появления на российском рынке: июнь 2012 г.
Подробная информация: http://kbpm-ib.ru/punktms
Фирма, предоставившая информацию: КБПМ – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ООО

См. стр. 40, 41

Программно-аппаратный комплекс "Однонаправленный шлюз-1" ПАК "Шлюз-1"

Производитель: ООО "КБПМ – информационная безопасность"
Сертификат: положительное заключение ФСБ на использование
Назначение: организация однонаправленной передачи информации из сегмента ЛВС, подключенного к Интернету (открытый сегмент), в сегмент ЛВС, в котором происходит обработка и хранение информации ограниченного пользования (закрытый сегмент)
Особенности: обеспечение однонаправленного канала передачи на физическом уровне (отсутствие обратного канала)
Возможности: скорость передачи информации составляет 1 Гбит/с
Характеристики: сетевые интерфейсы 1000 Base-TX-SC, 10/100/1000 Base-TX-RJ-45, сетевая среда
Ориентировочная цена: 400 000 руб.
Время появления на российском рынке: июнь 2012 г.
Подробная информация: http://kbpm-ib.ru/odnsh
Фирма, предоставившая информацию: КБПМ – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ООО

См. стр. 40, 41

Защищенный микрокомпьютер МКТ+

Производитель: ООО "Trusted Cloud Computers"
Сертификат: изделие подлежит сертификации
Назначение: работа в защищенном режиме с использованием мобильного устройства малого размера и любого имеющегося в наличии монитора, проектора или телевизора через HDMI или DVI (например, работа с ДБО или иными критичными к защищенности сервисами)

Особенности:
- ненастраиваемый клиентский компьютер
- защищенная ОС находится в разделе памяти, физически переведенном в режим RO; это гарантирует ОС от любых несанкционированных изменений
- в отличие от варианта МКТ, МКТ+ больше по размеру, но зато может обновляться в удаленном режиме по специально разработанной защищенной процедуре

Возможности:
- установка VPN-соединения из доверенной среды
- поддерживает управление проводными (USB) и беспроводными (2,4 ГГц, bluetooth) мышками, клавиатурами и пультами, работа с защищенными ключевыми носителями по протоколу CCID

Характеристики:
- питание от USB-порта телевизора или монитора, либо внешнего блока питания (5 В, 2 А)
- подключение к Интернету по Wi-Fi
- ОС Linux собственной сборки

Ориентировочная цена: 6800 руб.
Время появления на российском рынке: IV квартал 2014 г.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО

См. стр. 44, 45

Защищенный микрокомпьютер МКТ-card

Производитель: ООО "Trusted Cloud Computers"
Сертификат: изделие подлежит сертификации
Назначение: доверенный облачный микрокомпьютер с динамически изменяемой архитектурой

Особенности:
- конструктивно оформлен как док-станция с отчуждаемым компьютером
- к док-станции подключается периферия, питание и сеть
- док-станция инвариантна к отчуждаемой части (любой отчуждаемый компьютер может использоваться с любой док-станцией той же модели)

Возможности:
- док-станция содержит 8 USB-портов, выход HDMI, сетевой разъем RJ-45, разъем питания
- док-станция коммутируется с периферийным оборудованием через USB, с монитором через HDMI, с сетью – через RJ-45; возможно также использование Wi-Fi при условии разрешения на его применение

Характеристики: параметры компьютера аналогичны остальным решениям линейки МКТ
Ориентировочная цена: 8000 руб.
Время появления на российском рынке: IV квартал 2014 г.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО

См. стр. 44, 45

Защищенный микрокомпьютер МКТ-card long

Производитель: ООО "Trusted Cloud Computers"
Сертификат: изделие подлежит сертификации
Назначение: доверенный облачный микрокомпьютер с динамически изменяемой архитектурой

Особенности:
- отличается от МКТ-card только геометрическими пропорциями
- активная часть компьютера размещается в отчуждаемом модуле размерами 120x40x10 мм, что позволяет хранить его в стандартном пенале для ключей

Возможности: полностью аналогичны МКТ-card
Характеристики: полностью аналогичны МКТ-card
Ориентировочная цена: 8000 руб.
Время появления на российском рынке: IV квартал 2014 г.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО

См. стр. 44, 45

Услуги

Автоматизация процессов управления ИБ (IT GRC)

Отрасль: любая
Регион: РФ, Казахстан, Украина
Описание:
- компания предлагает услуги по автоматизации процессов управления информационной безопасностью в части:

– оценки соответствия (внутренний аудит) по требованиям нормативно-правовых актов РФ и внутренним требованиям по ИБ
– оценки уровня зрелости организационных и технических мер по ИБ
– оценки и обработки рисков ИБ
– оценки экономической эффективности от реализации проектов по ИБ или реализации конкретных мер защиты (ROSI)

- в качестве методологической базы по проведению вышеуказанных оценок при-

меняются собственные авторские методики, разработанные на базе лучших мировых практик (CRAMM, ISO 27001, ISO 27002, ISO 27005, COBIT и др.)
- используемые средства автоматизации проведения данных оценок построены по принципу "конструктора", позволяющего:

– производить гибкую настройку и адаптацию методик под конкретную компанию с учетом требований конкретной отрасли
– встроить процессы управления ИБ в общую систему корпоративного управления компании (в части управления рисками и внутреннего аудита)

- при необходимости возможна интеграция с внешними системами (SIEM, CMDB, сканерами безопасности) для получения актуальных данных о состоянии ИБ компании и использовании их для проведения вышеуказанных оценок
- стоимость проекта от $200 000

Фирма, предоставившая информацию: АСТЕРОС ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ГРУППА АСТЕРОС)

См. стр. 10, 11

Создание Центра оперативного управления информационной безопасностью компании (Security Operation Center)

Отрасль: банки, страховщики и финансовые организации, телекоммуникационные компании, энергетический сектор, нефтяные компании, промышленность, компании оптовой и розничной торговли, государственный сектор
Регион: РФ, Казахстан, Украина

Описание:
- компания предлагает клиентам услуги по созданию Центров оперативного управления информационной безопасностью компании, позволяющие автоматизировать и интегрировать в единую автоматизированную систему следующие процессы:

– мониторинг и регистрация критичных событий ИБ
– управление инцидентами ИБ
– управление уязвимостями ИТ-инфраструктуры
– оценка уровня соответствия требованиям по ИБ
– управление рисками ИБ
– оценка уровня зрелости процессов ИБ
– оценка ROSI от внедряемых мер защиты
– управление активами ИБ
– управление конфигурацией
– мониторинг работоспособности и производительности средств защиты
– контроль эффективности выполняемых процессов ИБ

- компания предлагает полный спектр услуг от разработки концепции создания Центра оперативного управления ИБ, разработки соответствующих процессов обеспечения и управления ИБ до автоматизации данных процессов и разработке единого информационно-аналитического портала, позволяющего в режиме реального времени отслеживать все показатели текущего состояния ИБ в компании в различных разрезах и с различной степенью детализации
- стоимость проекта от $200 000

Фирма, предоставившая информацию: АСТЕРОС ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ГРУППА АСТЕРОС)

См. стр. 10, 11

Разработка стратегии информационной безопасности

Отрасль: любая
Регион: РФ, Казахстан, Украина
Описание:
- сбор исходных данных для разработки стратегии ИБ (определение заинтересованных стороны, формирование рабочей группы, анализ существующих стратегий с точки зрения их влияния на ИБ, анализ потребностей бизнеса и текущего состояния ИБ на основе оценки соответствия ИБ требованиям законодательства, регуляторов, best practices, результатам внутренних и внешних аудитов, выявление и анализ факторов внутренней и внешней среды, оказывающих влияние на обеспечение ИБ, BIA-анализ и т.д.)
- разработка стратегии ИБ (определение стратегических целей обеспечения ИБ, определение стратегических задач и инициатив по обеспечению ИБ для перехода из текущего состояния в целевое и соответствующих им показателей, определение получаемых выгод от реализации стратегических инициатив, согласование стратегии ИБ со всеми заинтересованными сторонами и утверждение руководством)
- разработка плана реализации стратегии ИБ (формирование портфеля проектов ИБ, оценка и приоритизация проектов ИБ, разработка "дорожной карты" реализации стратегии ИБ по годам, разработка агрегированной оценки инвестиций в ИБ по годам)

Фирма, предоставившая информацию: АСТЕРОС ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ГРУППА АСТЕРОС)

См. стр. 10, 11

АЛАДДИН Р.Д.
129226 Москва,
ул. Докукина, 16, корп. 1,
этаж 7
Тел.: (495) 223-0001
Факс: (495) 646-0882
E-mail: aladdin@aladdin-rd.ru
www.aladdin-rd.ru
См. ст. "Биометрическая идентификация нового поколения от "Аладдин Р.Д." – концепция Match-on-JaCarta" на стр. 47

АМТ-ГРУП, ЗАО
115162 Москва,
ул. Шаболовка, 31б, подъезд 3
Тел.: (495) 725-7660
Факс: (495) 725-7663
E-mail: info@amt.ru
www.amt.ru
См. стр. 27

АСТЕРОС ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ГРУППА АСТЕРОС)
109052 Москва,
ул. Новохохловская, 23, стр. 1
Тел.: (495) 787-2450
Факс: (495) 787-2489
E-mail: info@asteros.ru
www.asteros.ru
См. ст. "Стратегический подход к трансформации" на стр. 10, 11

КБПМ – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ООО
107370 Москва,
Открытое ш., 12, стр. 1
Тел.: (495) 984-9711
Факс: (495) 984-9711
E-mail: kbpmib@kbpm-ib.ru
www.kbpm-ib. ru
См. ст. "К вопросу обнаружения компьютерных атак и вредоносного заражения" на стр. 40, 41

ОКБ САПР, ЗАО
115114 Москва,
2-й Кожевнический пер., 8
Тел.: (499) 235-6265
Факс: (495) 234-0310
E-mail: okbsapr@okbsapr.ru
www.okbsapr.ru,
www.accord.ru,
www.shipka.ru,
www.proSecret.ru,
www.proTerminaly.ru,
www.accord-v.ru, www.марш.рф
См. ст. "О действенных методах защиты съемных носителей" на стр. 44, 45

СМАРТ ЛАЙН ИНК, ЗАО
107140 Москва,
1-й Красносельский пер., 3,
пом. I, комната 17
Тел.: (495) 647-9937
Факс: (495) 647-9938
E-mail: support@devicelock.com
http://devicelock.com/ru
www.smartline.ru
См. ст. "Резидентные модули OCR в хостовых DLP-системах: новый уровень защиты от утечек данных" на стр. 34, 35

СПЛАЙН-ЦЕНТР, ЗАО
105005 Москва,
ул. Бауманская, 5, стр. 1
Тел.: (495) 580-2555
E-mail: cons@debet.ru
www.debet.ru, сплайн.рф
См. стр. 23

DNA DISTRIBUTION
115114 Москва,
ул. Дербеневская, 1, стр. 1
Тел.: (495) 228-0005
Факс: (495) 228-0006
E-mail: info@dnadis.ru
www.dnadis.ru
См. стр. 43

Groteck
Business Media

ИЗДАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВСЕГДА НА РАБОЧЕМ СТОЛЕ IT-СПЕЦИАЛИСТА

ПОДПИСКА НА ЖУРНАЛЫ:
Во всех отделениях почты России

Офисная подписка:
E-mail: monitor@groteck.ru
Тел.: (495) 6470442, доб.22-82

Информационное агентство
Монитор

Подписка:

expo.itsec.ru

INFOSECURITY RUSSIA' 2015

Выставка InfoSecurity Russia. 2015
обеспечивает максимальную полезность визита для заказчика и наивысший в России ROI для экспонента.

Приём заявок на участие открыт:
www.infosecurityrussia.ru

Событие №1 для IT директоров и руководителей служб информационной безопасности, государственных и коммерческих заказчиков.

infosecurity RUSSIA

Groteck Business Media