ЗАЩИТА ИНФОРМАЦИИ В «КИСАХ»: как противостоять киберугрозам

Марина ГРАМИНА,
Карина КОРОЛЕНОК

На данный момент в мире зарегистрированы тысячи предприятий и крупных корпораций. В связи с этим стремительно увеличиваются потоки входящих и исходящих данных, с невероятной скоростью растут объемы баз данных и архивов. Соответственно, возникает вопрос о целостности и защите информационных инфраструктур. В условиях активной информатизации всех сфер рыночной деятельности актуальность приобретает вопрос о защите непрерывно обновляющихся данных. Как следствие, возникает необходимость предотвращения и предупреждения кибератак в корпоративные информационные системы (КИС). В связи с этим был проведен анализ основных методов обеспечения безопасности сведений, которыми располагает та или иная организации, на примере белорусского центра разработок IBA Group.

IT-РИСКИ ВСЕ РАЗНООБРАЗНЕЕ

Информационные риски – это угроза, в результате которой возникают убытки или компания несет ущерб из-за использования информационных технологий. В то время как информацию уже давно оценили как ценный и важный актив, рост знаний в экономике вынудил организации становиться все более зависимыми от информации, от обработки информации и, особенно, от информационных технологий. Поэтому различные события или инциденты, которые ставят под угрозу IT каким-либо образом, могут оказывать неблагоприятное воздействие на бизнес-процессы организации, начиная от несущественного до катастрофического по своим масштабам.

Организации вынуждены создавать IT-отделы для того, чтобы поддерживать экономический процесс и эффективность управления компанией. Это вынуждает ведущие организации пересмотреть и трансформировать свою традиционную модель IT риск-менеджмента. В то время как стоимость является вызовом извлечения риск-менеджеров в организации, интегрированный IT-риск-менеджмент может существенно помочь улучшить бизнес. Высококвалифицированная команда IT-менеджеров позволяет своевременно принимать правильные решения и является первостепенным средством защиты в рамках организации.

Понимание сложной бизнес-среды и изменений внутри организации является одним из ключевых факторов в области риска компании. Эти факторы обеспечиваются за счет многочисленных сил, будь то внешние, такие как нормативные, геополитические, экономические, или внутренние, такие как создание новых продуктов.

Роль управления IT-рисками в организации трансформировалась в связи с быстрым ростом технологий и больше не рассматривается как простая поддержка бизнеса. Управление IT-рисками

также позволяет организациям дифференцировать себя и создает для них конкуренцию. В результате представление об управлении IT-рисками в рамках организации также эволюционировало. Поскольку IT-риски охватывают многие аспекты организации, предполагается, что функции внутреннего аудита, бизнес-операций и технологические операции будут иметь возможность прохождения мониторинга для устранения рисков. Функция управления IT-рисками поддерживает предприятие в целом. Она включает в себя решение стратегических задач и бизнес-модель организации. Эффективное управление IT-рисками обеспечивает надежное взаимодействие с контролирующими органами для определения приоритетов для каждой юрисдикции. Кроме того, от организации требуется предоставление возможностей, которые должны быть внедрены и управляемы через устойчивый процесс, чтобы обеспечить прозрачность и подотчетность. Целостный взгляд и обсуждение риск-менеджмента в IT-сфере помогают руководству определять, управлять и оптимизировать риски. Также благодаря автоматизации платформы функция управления IT-рисками обеспечивает серьезный контроль внутреннего аудита.

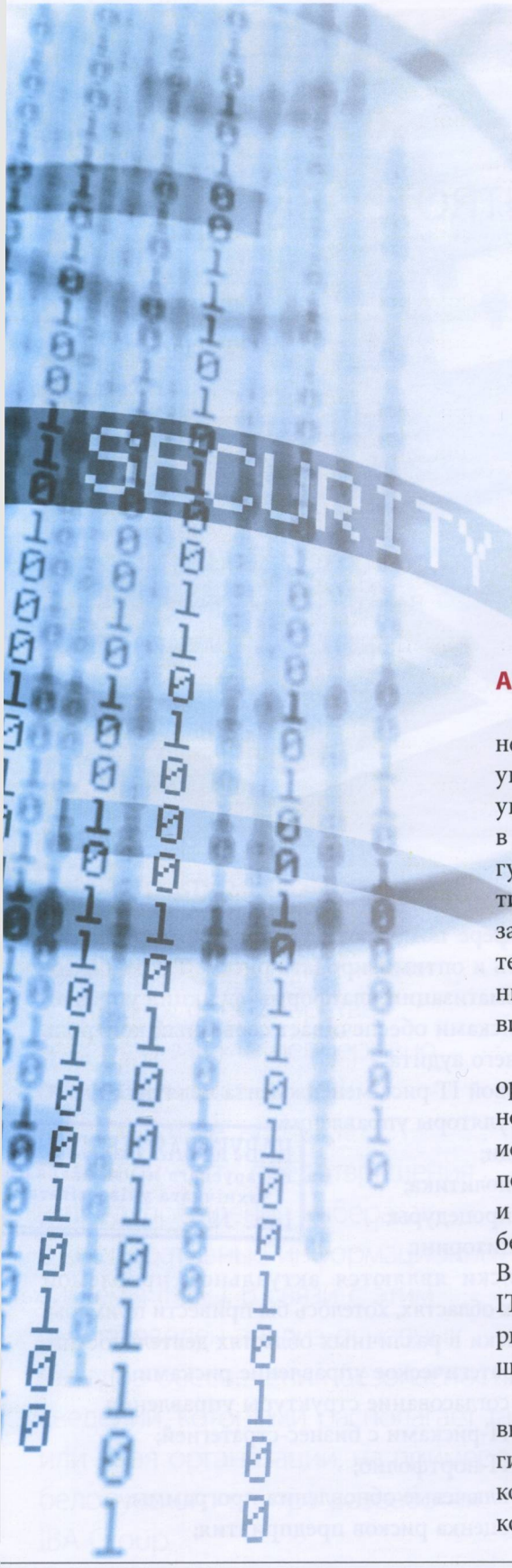
Основой IT-риск-менеджмента являются:

- регуляторы управления;
- люди;
- IT-политика;
- IT-процедуры;
- мониторинг.

IT-риски являются актуальной проблемой во многих областях, хотелось бы привести примеры.

IT-риски в различных областях деятельности:

1) стратегическое управление рисками:
   - согласование структуры управления IT-рисками с бизнес-стратегией;
   - IT-портфолио;
   - ключевые обновления программы;
   - оценка рисков предприятия;



2) соответствие нормативным требованиям:
   - строгие правила;
   - нормативно-правовая неопределенность;
   - рост расходов на предмет соответствия;
3) защита данных:
   - масштаб (большие данные);
   - рост неструктурированных данных;
   - нарушения правил безопасности;
   - обеспечение непрерывности бизнеса и аварийного восстановления;
4) SMM:
   - риски безопасности и защиты бренда;
   - новые маркетинговые и бизнес-модели;
   - утечка данных и интеллектуальная охрана имущества;
   - управление удаленным доступом и связью;
   - управление разными устройствами в IT-сфере;
5) окружающая сетевая среда:
   - конфиденциальность и безопасность данных;
   - налоговые и нормативные вопросы для виртуального бизнеса;
   - новые модели для хранения данных.

А ЕСТЬ ЛИ У ВАС РИСК-МЕНЕДЖМЕНТ?

На данный момент не в каждой компании существует система непрерывного риск-менеджмента в IT, т.к. полнофункциональное управление IT-рисками требует больших инвестиций. Системы управления IT-рисками популярны сегодня в индустрии связи, в сфере банковских и финансовых услуг. Эти отрасли жестко регулируются государством, а требования многочисленных нормативных актов постоянно повышаются, что отчасти продиктовано заботой о защите частной информации. Однако многие руководители компаний других отраслей уже осознали важность управления IT-рисками и стремятся учитывать связь между различными видами бизнес- и IT-рисков.

Процесс непрерывного управления IT-рисками для многих организаций может оказаться избыточным с точки зрения соотношения «стоимость-полезность». Для решения данной проблемы используют системы, основанные на дискретном подходе. Такой подход позволяет идентифицировать наиболее весомые риски и выбрать приемлемую стратегию управления для каждого из них без существенных затрат материальных и человеческих ресурсов. В то же время достигается основная цель системы управления IT-рисками – предоставление адекватной и достоверной оценки рисков, пригодной для принятия взвешенных управленческих решений бизнес-менеджментом.

В Республике Беларусь системы управления IT-рисками активно внедряются в банковской сфере. ОАО «Центр банковских технологий» при поддержке Национального банка разработан технический кодекс установившейся практики в области управления IT-рисками, который регламентирует применение процессного подхода для со-

здания, реализации, контроля, анализа, поддержания и совершенствования системы управления рисками в сфере банковских информационных технологий.

На данный момент в Республике Беларусь успешно развивается инфраструктура. Таким образом, большинство организаций имеет сеть, которая постоянно будет расширяться и обновляться, т.е. компоненты сети будут изменяться, и ее программные приложения будут заменяться или обновляться в более новые версии. Кроме того, будут происходить кадровые изменения, в течение времени может изменяться и политика безопасности. Эти изменения означают, что новые риски будут поверхностными, а риски, ранее уничтоженные, могут снова стать проблемой. Таким образом, процесс управления рисками продолжается и развивается. Ключом к достижению успеха будут являться правильные программы управления рисками. Управление IT-рисками будет опираться на приверженность высшего руководства; полную поддержку и участие IT-команды; компетентность группы по оценке риска; осознание и сотрудничество членов сообщества пользователей.

ПЯТЬ КОМПОНЕНТОВ БОРЬБЫ

С развитием технологий, в частности, интернета, распространились нападения на корпоративные сети через Всемирную Паутину. Поэтому сотрудники компаний, отвечающие за сохранность данных, стоят перед задачей защиты конфиденциальной информации.

В результате было разработано 2 метода обеспечения защиты информации в корпоративных системах: IDS и IPS.

Первой была разработана IDS (Intrusion Detection Systems) – система обнаружения вторжений. Она позволяет администратору выявить угрозу чужеродного внедрения в сеть. За годы использования такой метод приобрел авторитет и доверие пользователей, однако со временем появился более эффективный способ защиты персональных материалов – IPS (IntrusionPreventionSystem) – система предотвращения вторжений. Данная система представляет собой набор технологий и средств, обеспечивающих не только уведомление о вторжении, но и, в отличие от IDS, его предотвращение. Среди разработок IPS можно выделить пять типов компонентов, каждый из которых выполняет свои функции и может комбинироваться с другими:

- **сетевая IDS.** Данное устройство изучает IP-пакеты с целью выявления угрозы атаки и в случае ее наличия блокирует все несоответствия;
- **коммутаторы седьмого уровня** – устройства, служащие либо для абсолютного уничтожения подозрительных пакетов, либо для их перенаправления на специальный сервер для повторного анализа;
- **экран приложений** отслеживает поведение программ и библиотек, работающих с сетью. Подобные экраны останавливают атаки, но при этом важно учитывать, что данный механизм требуется устанавливать на каждый персональный компьютер и проводить необходимые переустановки при каждом изменении конфигурации приложений;
- **гибридные коммутаторы** представляют собой механизм, объединяющий функции экранов приложений и коммутаторов седьмого уровня. Преимуществом является то, что они не только отражают атаки на отказ в обслуживании, но и могут предупредить о неизвестных атаках;
- **ловушки.** К категории IPS относятся такие ловушки, которые делают попытки активного вмешательства в нападение. Принцип работы таких продуктов заключается в том, чтобы спровоцировать нападающие программы на вторжение, одновременно контратакуя их, идентифицируя при этом их личность.

Важно отметить, что IPS разных типов могут успешно объединяться в довольно эффективную систему защиты, где каждый элемент взаимосвязанно работает с другим. Более того, разумеется, данные механизмы не конкурируют с уже существующими межсетевыми экранами, антивирусными программами и тому подобным, т.к. скорее дополняют их.

Тем не менее, несмотря на развитую систему защиты, аналитики задаются вопросами относительно того, насколько она совершенна. Проблема эффективности данных методов требует оценки не только разработчиков, но и существующих и потенциальных клиентов. Поэтому необходимо определить, в какой степени механизмы IPS могут справляться с поставленными задачами. Разумеется, в связи с постоянно растущими требованиями к устройствам защиты IPS определенно выигрывает на фоне IDS. Тем не менее сейчас все чаще и чаще пользователи испытывают затруднения в использовании IPS, т.к. оригинальные версии значительно отличаются от упрощенных.

ОБРАТНАЯ СТОРОНА «ИНТЕРНЕТА ВЕЩЕЙ»

Специалисты в области безопасности усердно работают над совершенствованием систем для профилактики предотвращения атак и прогнозируют слияние технологий IDS и межсетевых экранов, что могло бы только добавить преимущества данным средствам при обеспечении сохранности данных.

Работники компании Gartner, специализирующейся на рынке информационных технологий, предполагают, что следует воздержаться от крупных инвестиций в области IDS и вместо этого подробнее изучить принципы работы IPS, т.к. считают это направление более успешным и результативным. Перспективными они считают разработки компаний ArcSight и NetForensics. По мнению аналитиков, концепция IDS себя исчерпала: она не представляет сегодня практически никакой ценности для корпоративных пользователей. В современных условиях следует находить более оперативные и приспосабливаемые способы защиты внутрикорпоративных данных.

К одному из самых существенных недостатков IDS можно отнести ложные срабатывания, которые значительно обременяют работу. Эта проблема устранена в продуктах IPS, которые помогают избежать фальсификации угрозы. Во многом решить эту проблему помогают анализ сигнатур, изменяющихся в ходе проверки, или идентификация сетевых протоколов с целью обнаружения внезапных изменений в шаблонах трафика.

Однако необходимо отметить, что, вопреки усилиям производителей средств безопасности, такие системы не лишены брешей, что делает их значительно менее устойчивыми как к внешним, так и к внутренним угрозам. Ситуацию усугубляет то, что меры по восстановлению поврежденных систем весьма дорогостоящие. Корпоративные сети все чаще и чаще подвергаются вирусным атакам. Глобальные эпидемии Nimba, Klez, CodeRed вынуждают разработчиков интенсивно трудиться над созданием надежных методов.

Следует упомянуть, что некоторые клиенты по-прежнему относятся с недоверием к устройствам IPS, т.к. данный механизм работает автономно, т.е. принимает решения независимо от человека (даже в отношении сетевого трафика). Тем не менее преимущества IPS перед IDS очевидны.

С учетом того что в настоящее время атаке может подвергаться буквально любое устройство, вопрос защиты остается актуальным. К примеру, некоторые специалисты даже предполагают, что в ближайшее время будет неудивительно, если взлому подвергнутся системы даже при простом подключении… к принтеру.

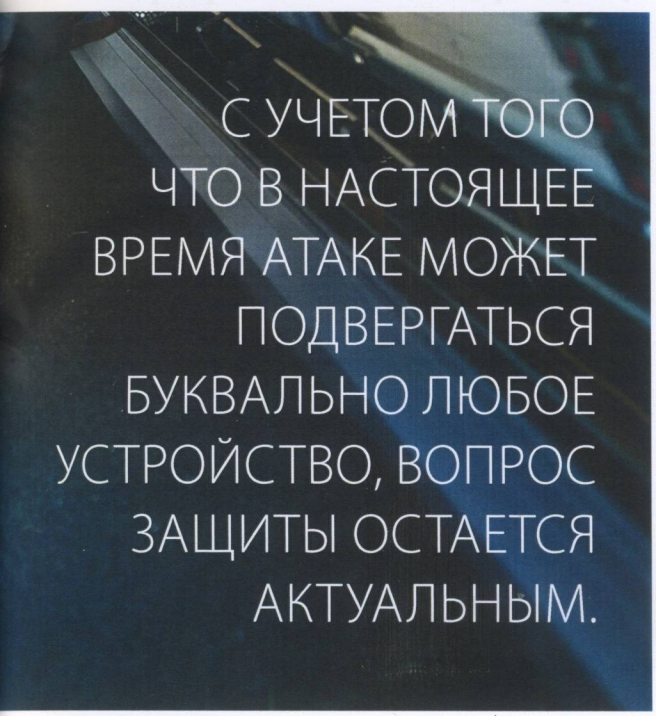
ДЕНЬ БЕЗОПАСНОСТИ: НА УРОВНЕ НАЦИОНАЛЬНЫХ ПРОГРАММ

В Беларуси в течение последних 5 лет самым серьезным DDoS-атакам (атаки, при которых программы крадут информацию) подвергались крупнейшие онлайн-СМИ, сайты госорганов, туристические сайты, а также сервера провайдеров интернет-услуг, вследствие чего был затруднителен доступ пользователей к различным страницам и сервисам.

К самым распространенным типам атак можно отнести, к примеру, следующие:

- **XSS** (англ. Cross Site Scripting – «межсайтовый скриптинг») – тип атаки на веб-системы, механизм действия которого заключается во внедрении в необходимую страницу вредоносного кода и в слиянии этого кода с веб-сервером злоумышленника. Эффективными средствами защиты против данного принципа вторжения являются периодический анализ безопасности кода и проверка на проникновение. Межсайтовый скриптинг может быть использован и для проведения DoS-атаки;

- **внедрение SQL-кода** (англ. SQL injection) – один из хорошо работающих способов взлома сайтов, в основе которого лежит внедрение в запрос произвольного SQL-кода. Атака типа внедрения SQL может быть возможна из-за некорректной обработки входных данных, используемых в SQL-запросах;



- **PHP Including** подразумевает внедрение произвольного php-кода в страницы сайта.

Информационная безопасность является одним из приоритетных направлений деятельности белорусских центров разработок IBA Group. Деятельность альянса IBA включает в себя создание комплексных решений для фирм, разработки систем безопасности предприятий, а также участие в национальных программах. IBA Group активно участвует в составлении широкого диапазона программ, обеспечивающих защиту информации.

IBA Group использует новейшие технологические достижения и программные продукты мировых лидеров в области информационной безопасности: компаний ArcSight, Check Point, Splunk, IBM Tivoli.

Более того, IBA Group, компании Check Point Software Technologies, Imperva и Splunk организуют традиционный семинар по информационной безопасности – IBA SecurityDay. Данное мероприятие создано с целью повышения уровня осведомленности основных заказчиков на рынке Республики Беларусь о новейших изменениях в технологиях и средствах борьбы с угрозами вторжения, нависающими над корпоративными информационными сетями и периметром безопасности предприятий в результате действия кибератак в сетях общего доступа (Internet). К тому же семинар направлен на раскрытие тем о средствах противостояния киберугрозам на базе решений IBA Group, создаваемых совместно и на основе серии продуктов мировых лидеров в создании технологий защиты.

Программа мероприятия включает в себя обзор продуктов Check Point, анализ внедрения систем управления полномочиями на примере белорусских банков, перечень способов зашиты от угроз нулевого дня, презентацию об управлении безопасностью поколения Check Point Security Management R80, ознакомление со спецификой лицензирования продуктов Check Point, детальный разбор средств защиты Web-приложений (WAF) от компании Imperva, изучение решений для построения BigDataSecurity.

Таким образом, с развитием технологий компаниям постоянно необходимо следить за сохранностью своей информации, а также за новейшими разработками в области защиты информации. На примере IBA Group мы убедились в том, что в Беларуси также развиваются технологии по защите информации в корпоративных информационных системах. Данный факт не может не радовать, т.к. это свидетельствует о прогрессе в нашей стране.