ФОРМИРОВАНИЕ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

ОСНОВЫ РАЗРАБОТКИ СИСТЕМ КОНТРОЛЯ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ

В.Е. Жужжалов, К.Л. Стоякова,
Р.Р. Ибраев, Д.Д. Ганин

Кафедра систем управления
Московский государственный университет технологий
и управления им. К.Г. Разумовского
ул. Земляной вал, 73, Москва, Россия, 109004

Статья посвящена анализу информационной безопасности в условиях быстроразвивающихся высокотехнологичных средств обработки информации и разработке систем защиты информации от внутренних угроз.

Ключевые слова: информационная безопасность, защита информации, информационные технологии, система контроля.

Опасности информационных систем — внешние угрозы: вирусы, хакерские атаки и спам, защита от которых осуществляется почти на каждом предприятии, и внутренние угрозы: саботаж, хищение данных, неосторожные действия сотрудников. Около 80% потерь, связанных с нарушением информационной безопасности, вызывается утечкой конфиденциальной информации, допущенной внутри компании.

Для того чтобы построить эффективную систему информационной безопасности, необходимы: четкое представление о том, что нуждается в защите; осведомленность о соответствующих угрозах; способность их предотвратить. Если ранее злоумышленники «атаковали» в большей степени малые и средние плохо защищенные компании, то теперь в поле их внимания крупные организации, владеющие огромными информационными базами. Они используют слабые места в технологиях и в бизнес-процессах. До сих пор системы ИТ-безопасности были похожи на глухие крепостные стены с тщательно охраняемыми входами. В нынешних условиях такая защита недостаточна, поэтому тактика была изменена. Для того, чтобы оставаться защищенной, компания должна быть *прозрачной*, чтобы ни один процесс не оставался за рамками мониторинга и контроля.

Корпоративные скандалы и массовые утечки информации приводят к внедрению новых законодательных норм и правил, и руководство компании вынуждено следить за соответствием многочисленным национальным и международным правовым актам. Тенденция прослеживается очень четко: если компания не предпринимает необходимых действий для обеспечения безопасности информации своих заказчиков, то результатом может стать потеря доверия, подрыв репутации, снижение стоимости акций, штрафы и, возможно, уголовная ответственность для ответственных руководящих лиц.

Информационная безопасность вышла за рамки процесса управления рисками, теперь она имеет статус фундаментального элемента ведения бизнеса. Количество внутренних атак в компаниях различных сфер бизнеса на сегодняшний день превышает количество внешних, причем рост количества внутренних атак за последний год более чем двукратный: с 14% от общего количества нарушений информационной безопасности в прошлом году до 35% в нынешнем. Самые распространенные из внутренних угроз — *неавторизированный доступ* в систему (сервер, персональный компьютер или базу данных), *неавторизированный поиск* или просмотр конфиденциальных данных и попытки обойти или взломать систему безопасности или аудита, *несанкционированные манипуляции с информацией* — изменение или уничтожение данных, а также сохранение или обработка конфиденциальной информации в системе, не предназначенной для этого.

Внутренние атаки на информационные системы наносят огромный ущерб, и не только финансовый: утечка конфиденциальных данных — это серьезный удар по репутации компании. Технически утечка может произойти по нескольким каналам: через почтовый сервер — с помощью электронной почты, через прокси-сервер — при использовании открытых почтовых систем, через принтер — при физической печати документов, через мобильные накопители различного рода — дискеты, CD-диски, переносные устройства с флеш-памятью и встроенным жестким диском. Угрозы со стороны собственного персонала нельзя предотвратить полностью, но ими можно управлять и свести к минимуму. При создании полномасштабной системы информационной безопасности следует учитывать все возможные способы совершения внутренних атак и пути утечки информации. Необходимы системы защиты, позволяющие контролировать информацию, проходящую через каждый узел сети, и блокировать все попытки несанкционированного доступа к конфиденциальным данным.

Защита каждой отдельно взятой станции и информационной системы в целом должна строиться на двух принципах: отключение сервисов, избыточных для пользователя; постоянный мониторинг ситуации в активных сервисах. Соблюдение баланса между этими двумя принципами — постоянный компромисс, но только так можно создать прозрачную и гибкую систему безопасности, одинаково эффективно защищающую от внешних и внутренних угроз. При создании полномасштабной системы информационной безопасности следует учитывать все возможные способы совершения внутренних атак и пути утечки информации.

Ядро современной системы безопасности — логическая основа управления рисками. Идентификация, анализ рисков и правила реагирования на реализован-

ные угрозы — все это составляет систему управления ИТ-инцидентами, в основе которой лежит принцип логической парадигмы.

Функции системы безопасности — фиксация факта нарушения политики информационной безопасности и оповещение о нем офицера безопасности, ранжирование инцидентов по степени критичности и определение регламентов реагирования на них, консолидация и хранение информации о произошедших инцидентах в масштабе всего предприятия и, наконец, ретроспективный анализ произошедших инцидентов позволяют:

— выявлять в исходящем потоке электронной почты (SMTP) сообщения, которые могут представлять угрозу утечки конфиденциальной информации, фильтровать сообщения, нарушающие политику информационной безопасности;

— выявлять в исходящем HTTP-потоке данные, которые могут представлять угрозу утечки конфиденциальной информации; фильтровать данные, нарушающие политику информационной безопасности;

— выявлять нежелательную активность пользователей в сети, которая может представлять угрозу утечки конфиденциальной информации, производить мониторинг на уровне файловых операций, оповещать об инцидентах в онлайн-режиме;

— контролировать использование мобильных устройств хранения информации, устройств передачи информации и коммуникационных портов;

— хранить почтовую корреспонденцию, систематизировать и контролировать историю корпоративной почтовой корреспонденции и производить ретроспективный анализ инцидентов утечки конфиденциальной информации.

Интегрированное решение обеспечивает конфиденциальность с возможностью централизованного управления и оповещения об инцидентах в режиме реального времени.

Системы контроля и защиты информации от внутренних угроз на основе элементов логической парадигмы (например, логические языки программирования) должны быть разработаны с учетом всех вышеперечисленных требований к их алгоритму функционирования. Они представляют собой сбалансированный набор средств для эффективного управления информационной безопасностью компании, без которого невозможно непрерывное ведение бизнес-процесса. При разработке систем контроля и защиты информации от внутренних угроз необходимо минимизировать финансовые риски, связанные с утратой конфиденциальности данных, а также привести информационную систему в соответствие с национальными и международными законами и стандартами.

Такая система является интегрированной, т.е. способна охватывать все уровни компании вплоть до принятия решений, которые обеспечивают контроль над наиболее распространенными путями утечки, мониторинг доступа сотрудников к корпоративным информационным ресурсам и хранение подробного архива операций с документами.

Основная особенность использования элементов логической парадигмы при разработке систем контроля и защиты информации от внутренних угроз — обработка информации в масштабе реального времени. Системы, работающие в режи-

ме реального времени, фильтруют почтовый и веб-трафик и контролируют операции с документами на рабочих станциях (местах), предотвращая вывод конфиденциальных данных за пределы информационной системы. В случае обнаружения фактов нарушения корпоративной политики ИТ-безопасности система оперативно сообщает об инциденте компетентным лицам и помещает подозрительные объекты в область карантина.

ЛИТЕРАТУРА

[1] *Конявский В.А., Лопаткин С.В.* Компьютерная преступность. В 2 т. Т. 1. — М.: РФК-Имидж-Лаб, 2006.
[2] Информационная безопасность систем организационного управления. Теоретические основы: Монография. В 2 т. — М.: Наука, 2006.
[3] *Ботт Э., Зихерт К.* Локальные сети и безопасность Microsoft Windows XP. Inside Out. — М.: Эком, 2007.

LITERATURA

[1] *Konjavskij V.A., Lopatkin S.V.* Komp'juternaja prestupnost'. V 2 t. T. 1. — M.: RFK-Imidzh-Lab, 2006.
[2] Informacionnaja bezopasnost' sistem organizacionnogo upravlenija. Teoreticheskie osnovy: Monografija. V 2 t. — M.: Nauka, 2006.
[3] *Bott Je., Zihert K.* Lokal'nye seti i bezopasnost' Microsoft Windows XP. Inside Out. — M.: Jekom, 2007.

THE BASES OF DEVELOPMENT OF SYSTEMS OF CONTROL AND PROTECTION INFORMATION FROM INTERNAL THREATS

V.E. Zhuzhzhalov, K.L. Stoyakova, R.R. Ibrayev, D.D. Ganin

Control systems chair
Moscow state university of technologies and managements of K.G. Razumovsky
Zemljanoj val str, 73, Moscow, Russia, 109004

The present article is devoted to the analysis of information security in the conditions of high-growth hi-tech means of information processing and information security development of systems from internal threats.

Key words: information security, information security, information technologies, monitoring system.