СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Скобелева С. Н., Дорогой Л. С.
Кафедра «Информационный и электронный сервис», Поволжский государственный университет сервиса
Тольятти, Российская Федерация
E-mail: skobeleva-sn@yandex.ru

Рассмотрены вопросы, связанные с разработкой стратегии информационной безопасности предприятия

Введение

В современном мире предприятия все чаще сталкиваются с необходимостью уделять особое внимание обеспечению информационной безопасности и инвестировать в неё средства. Риски, возникающие в процессе ведения бизнеса, окружают компании со всех сторон. Широкое распространение ИТ технологий, социальных сетей, персональных мобильных устройств, способствовало появлению качественно нового уровня угроз. Компании могут просто принять этот факт и продолжать работать в надежде, что угрозы их не затронут. Они также могут попробовать внедрить ряд ответных мер, пытаясь снизить эти риски или нанять специализированную компанию, которая будет заниматься обеспечением информационной безопасности. Можно вообще избежать всех рисков, просто закрыв предприятие и прекратив бизнес активность. Информационная безопасность базируется на трех основных принципах: доступности, целостности и конфиденциальности. Существует множество стандартов и лучших практик по информационной безопасности, среди которых ISO27000, COBIT 5, NIST SP 800, COSO и др. Однако, в каждой отрасли есть свои особенности, которые необходимо учитывать, внедряя тот или иной стандарт.

I. Исходные данные

При разработке стратегии информационной безопасности необходимо, опираясь на поддержку высшего руководства компании, разработать политики и процедуры с учетом организационных особенностей, проводить обучающие мероприятия сотрудников компании, идентифицировать и управлять рисками, быть уверенными в соответствии требованиям регуляторов, а также своевременно обнаруживать и предотвращать инциденты. Вся информация в компании должна быть классифицирована по типам: для публичного доступа, для частного доступа (политики, внутренние документы) и конфиденциальная (финансовые отчеты, ноу-хау, разработки, данные о клиентах). Важную роль в разработке стратегии информационной безопасности играет политика информационной безопасности. Высшее руководство компании определяет политику информационной безопасности, соотнеся ее со стратегическими целями компании. Политика информационной безопасности должна учитывать существующее законодательство, предписания регулирующих органов (например, обеспечение защиты персональных данных). Политика информационной безопасности определяет видение и стратегию обеспечения непрерывности бизнес процессов компании. Политика информационной безопасности должна опираться на стандарты и процедуры, разработанные в компании. Также она определяет степень терпимости высшего менеджмента к различного рода рискам. Политику информационной безопасности, основанную на бизнес целях, необходимо разработать, напечатать и донести до всех сотрудников компании. Если сотрудники не подписывают документы с требованиями, это значит, что они не обязаны следовать политике информационной безопасности. Следовательно, компания не может требовать от них ее исполнения. Политика должна регулярно обновляться с учетом потребностей компании

II. Разработка стратегии информационной безопасности

Стратегия информационной безопасности компании должна предусматривать разработку и внедрение контрольных процедур (механизмов контроля). Они подразделяются на три типа: Административные – Процедуры, политики, нормативные документы, которые подписывают сотрудники перед исполнением служебных обязанностей в компании, обычно в первый день приема на работу. Здесь может быть сказано, что нельзя пересылать личные сообщения через рабочую электронную почту, использовать корпоративный мобильный телефон для личных звонков, а также пользоваться Интернетом только в служебных целях. Работодатель будет иметь право отслеживать активность пользователя, который с этим соглашается. Если пользователь не подписал такое соглашение, то компания юридически не в праве требовать соблюдения этих требований. Технические (логические) – Логические механизмы контроля могут быть реализованы на базе оборудования, систем обнаружения угроз, правил на маршрутизато-

рах и коммуникационном оборудовании, прокси серверах, а также на уровне операционных систем Windows, Linux – путем разграничения прав доступа определенных категорий пользователей. Технические механизмы контроля должны опираться на административные, чтобы работать корректно. Например, финансовый директор подписывает заявку на матрицу доступа для сотрудников финансового департамента, на тип доступа к определенным папкам и документам. Затем, сотрудник департамента ИТ на основании заявки выполняет необходимое разграничение прав доступа учетных записей пользователей в Active Directory. Физические механизмы контроля – Огороженная территория, охрана, замки, системы контроля доступа, магнитные карты, биометрические сканеры, датчики движения, серверные комнаты со специализированным оборудованием, детекторы дыма, системы автоматического пожаротушения. Комбинации таких механизмов контроля позволяет создавать эффективную защиту от ошибок и неправомерных действий. Кроме того, контрольные процедуры делятся на превентивные, обнаруживающие и корректирующие, примеры которых показаны ниже. Перед тем как совершить транзакцию на сумму от 10 000 долларов сотрудник банка должен получить согласование менеджера (административные меры контроля), поскольку программное обеспечение не позволяет ему самостоятельно осуществить такую транзакцию (элемент логического контроля по разделению прав доступа). Транзакцию можно осуществить только с рабочего места пользователя, находящегося в бизнес центре под охраной (элемент физического контроля). Это механизм превентивного контроля. В качестве обнаруживающих контрольных процедур на административном уровне используется периодический ИТ аудит, на техническом уровне - системы контроля вторжений (IDS) или специальные серверы, отслеживающие вторжения в сеть предприятия (Honeypot). На физическом уровне такими мерами могут служить датчики движения, датчики температуры и влажности в серверных помещениях. Механизм корректирующего контроля можно проиллюстрировать на примере. На рабочем месте пользователя с помощью антивирусного ПО был обнаружен компьютерный вирус, сотрудник уведомляет об инциденте непосредственного руководителя и департамент ИТ. Компьютер изолируется (физически отключается от компьютерной сети или по питанию) и с ним производятся действия по восстановлению. В каждой отрасли промышленности есть свои стандарты, требования и регулирующие документы. Например, для банков и платежных систем существует Payment Card Industry Data Security Standard (PCI DSS), а для медицинских учреждений – закон по защите персональных данных пациентов. Если предприятия не соблюдают эти требования, то это может иметь серьезные негативные последствия для их бизнеса. Предприятия подвергаются целому ряду угроз, в связи с попытками злоумышленников получения несанкционированного доступа к информационным активам. Широкое распространение получили Dos-атаки на серверы и сетевое оборудование компании, спам, изменение e-mail сообщений, фарминг-атаки, анализ трафика, сканирование Wi-Fi сетей, прослушивание телефонных переговоров, вирусные атаки, вызов удаленных процедур и др. По типу воздействия это могут быть хакеры, текущие и бывшие сотрудники компании, персонал службы ИТ, подрядчики и временные сотрудники по контракту. Согласно исследованию компании “Infowatch”, более 70% сотрудников ИТ-служб и более 85% сотрудников ИБ-служб не уверены, что системы обеспечения информационной безопасности в их компаниях защищают их от внутренних угроз. Аудиторы информационных систем особое внимание обращают на риски, связанные с разделением обязанностей (SoD) в компании. В частности, нельзя зависеть только от одного ключевого сотрудника, все функции рекомендуется дублировать, а если это не представляется возможным, то обеспечить меры компенсационного контроля. При разработке стратегии информационной безопасности предприятия необходимо уделить внимание резервному копированию данных и иметь план ликвидации последствий возможных непредвиденных действий и катастроф. Землетрясения, наводнения, военные действия, ураганы, пожары в один момент могут уничтожить критически важную информацию. В связи с этим центры обработки данных, согласно лучшим практикам, должны находиться в географически удаленных объектах, странах, что существенно повышает вероятность сохранения критически важных данных для компании.

Заключение

В современных условиях обеспечение информационной безопасности требует комплексного подхода, учета, казалось бы, не относящихся к ИТ факторов и рисков. По мере развития информационных технологий риски, связанные с их применением, тоже будут возрастать, и высшее руководство компаний должно быть к этому готово, уделяя особое внимание разработке стратегии информационной безопасности.

1. Shon Harris, Fernando Maymi CISSP® All-in-one Exam Guide, Seventh Edition. – McGraw-Hill Education, USA. – 2016. – 1341 p, ISBN 978-0-07-184961-6.
2. Аналитический Центр InfoWatch Безопасность информации в корпоративных информационных системах. Внутренние угрозы. – URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch Report 2013 ugroz.pdf (дата обращения: 30.03.2017).