ДИРИЖЕР СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Олег СОЛОНЕНКО,
Экономическая Академия Молдовы

In the paper analyzed requirements for building the information security system

Введение

По мнению экспертов в области информационной безопасности и в аналитических отчетах крупных брендов говориться о том, что самым слабым звеном в любой системе безопасности является человеческий фактор. Это значит, что построение системы управления информационной безопасности (СУИБ) необходимо начинать с человека, причем с человека, который будет эту систему строить и заботиться о ее каждодневной работе.

Профиль компетентности Офицера информационной безопасности

Найти офицера информационной безопасности является самой настоящей проблемой по причине несформированности профиля компетенции и отсутствия подготовленных специалистов. Главная его задача - это оценка и управление технологическими, производственными и иными рисками компании в срезе информационной безопасности. Предполагается, что данный специалист должен быть способен идентифицировать риски и управлять ими в соответствии с целями и задачами компании и уровнем ее развития. По-видимому, он будет входить в верхний эшелон управления компанией, чтобы иметь возможность сбалансировать потребности бизнеса и требования безопасности с учетом усложняющихся технологий, возросшего числа действий злоумышленников, требований законодательства и ожиданий партнеров. В дополнение к солидному образованию и опыту в области защиты информации он, несомненно, должен обладать стратегическим складом ума, познаниями в управлении предприятием и лояльностью к компании.

Есть несколько путей замещения вакантной позиции. Один заключается в заполнении этой позиции аудиторами или аналитиками в области безопасности. Проблема в том, что хороший аналитик и хороший управленец - не одно и то же. Это люди с принципиально разным складом ума, структурой мотивации и компетентностью, для совмещения в этом случае нужно учить и укреплять его по менеджерской составляющей. Второй путь - привлечение готового или почти готового специалиста из числа своих же сотрудников. В этом случае профессиональная компетенция будет усилена еще и знанием конкретного производства. [1]

С одной стороны, для офицера информационной безопасности необходимы знания таких понятий, как ACL, DES,VPN, с другой стороны ROI, SLA, бизнесс процессы. Не плохо бы иметь высшые образования в области: электротехники, информатики, экономики, психологии.

Построение системы информационной безопасности

Построение информационной безопасности в организации не стоит в списке задач под номером один. Существуют отдельные технические и программные средства – иначе организация больше простаивает, чем работает, но все это приобретенный опыт предыдущих лет [2]. И тут возникает серьезный инцидент или внешнее воздействие в виде закона (либо требования) – и тогда возникает потребность в построении системы способной реагировать на такие воздействия.

Самый простой способ возложить все на плечи ИТ. Если строить информационную безопасность снизу то при особом умении, каждый пользователь системы будет отвечать за состояние информации, не имея необходимых для этого инструментов. Может дойти до абсурда, когда собственнику информации необходимо доказывать право на доступ к ней. Организация при этом делиться на "Админов" (доступ ко всей информации) и "юзеров" (доступ к той ее части, к которой доступ получен в результате долгих хождений, многих подписей и изматыванием нужных админов) - и при этом топ-менеджмент в группе юзеров. Информация живущая за пределами ИТ систем – на бумаге или в вербальном виде живет своей отдельной жизнью.

Другая сторона медали – построение информационной безопасности сверху. Политика, процедуры, инструкции – все есть. Мы получаем красивую глянцевую обложку, можно даже с аудитом и с необходимыми сертификатами по безопасности. Кто-то видел в аудиторском заключении Ernst&Young, KPMG, PWC, строку о том, что в ИТ инфраструктуре организации найден сервер с игрой "Counter-Strike" где отдел маркетинга сражается с системными администраторами (и те и другие люди креативные), а на серверах организации собрана самая большая (после хостинговых и торентовых серверов) коллекция музыки от классики до хауса и последние фильмы (даже не вышедшие в прокат)? Программисты занимаются взломом чужих программ и изучением алгоритмов игр, в оболочке игры от первого лица - для "повышения своего профессионального уровня".

Понятно, что тот, кто платит, тот и заказывает музыку. А ответ лежит в области вычисления интеграла с пределами от 0 до беконечности. Думаю, что нужно сузить область. Нужно строить живой организм похожий на нейронные сети, которые отличаются от компьютера тем, что в них нет процессора, и они не хранят информацию в централизованной памяти. Знания и память сети распределены по ее соединениям. А офицер информационной безопасности не центральный процессор, а скорее маршрутизатор подбирающий путь с наименьшей стоимостью.

Люди – это главное, что определяет успех

Сейчас почти никого не нужно убеждать в том, что люди мотивированные, обученные, обладающие необходимыми для данной работы и данной организации компетенциями, в очень большой степени определяют успех бизнеса. Почти не осталось монопольных рынков, любое "ноу-хау" быстро подхватывают конкуренты, поэтому чаще всего теперь побеждает тот, у кого лучше команда. Известно, что характер человека включает в себя много качеств, таких как жизненный опыт, уровень интеллекта, социальный слой и среда, образование, пол, состояние здоровья, в том числе и психи-

ческого, темперамент, генотип и многое другое. Существует множество подходов к подбору и оценке персонала – необходимо рассматривать и применять те методики, которые выдержали испытание практикой и показали свою эффективность, что позволит использовать их для создания оптимальной систему оценки и мотивации персонала.

Выводы

Информационной безопасности – это синергия таких областей как математика, информатика, экономика, кибернетика, психология. "Один в поле не воин" – поэтому задача офицера информационной безопасности построить систему, в которую вовлечены все участники информационного пространства. Не стоит забывать о том, что со временем офицер информационной безопасности будет владеть объемом информации большим, чем кто-либо другой в организации [3].

Литература

1. Марк Розин – "Советы консультанта: Аутсорсинг до абсурда" [Электронный ресурс] - http://www.vedomosti.ru/newspaper/article/254596/autsorsing_do_absurda
2. А. Голов, В.Кузнецов - "Практический подход к построению системы управления ИБ" [Электронный ресурс] - http://www.topsbi.ru/default.asp?artID=903
3. Брюс Шнайер - "Психология безопасности" [Электронный ресурс] - http://www.securitylab.ru/analytics/350910.php
4. Статья "Хакер в столовой" - Электронный журнал "Хакер" [Электронный ресурс] - http://www.xakep.ru/post/35784/default.asp

ОЦЕНКА РИСКОВ, ВОЗНИКАЮЩИХ ПРИ ВНЕДРЕНИИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Наталья ГРИГОРЬЕВА,
Антон ШУТОВ,
Денис ГРАДУСОВ,
Владимирский государственный университет (Российская Федерация)

The article addresses issues related to the assessment of risks arising from the implementation of corporate information systems. It is proposed risk assessment using fuzzy sets theory.

Декларируемые разработчиками корпоративного программного обеспечения выгоды и преимущества, получаемые в результате приобретения конкретной корпоративной информационной системы, проявятся только в случае ее успешного внедрения. Проект внедрения является сложным, многоэтапным процессом, связанным со значительными изменениями на предприятии и часто сопровождающимся различными трудностями и рисками. Поэтому при внедрении корпоративных информационных систем важно управлять рисками, которые необходимо заранее определять и оценивать. Своевременное определение рисков и связанных с ними факторов, позволит устранить недостатки проекта, тем самым повысив его эффективность.