УО «Алматы Менеджмент Университет»

МЕНЕДЖМЕНТ БИЗНЕС АНАЛИТИКА

Выпуск 3

Алматы, 2016

УО «Алматы Менеджмент Университет»
Высшая Школа Бизнеса

МЕНЕДЖМЕНТ. БИЗНЕС. АНАЛИТИКА

Сборник статей слушателей программы MBA
Выпуск 3

Алматы, 2016

УДК 005:378
ББК 65.290-2:74.58
М50

Все статьи прошли проверку на уникальность текста в системе Антиплагиат.ру (не ниже 60%).

Менеджмент. Бизнес. Аналитика. Сборник научных статей слушателей программы MBA. - Алматы: Алматы Менеджмент Университет, 2016. – 340 с.

ISBN 978-601-7166-12-0

Настоящий сборник предназначен для студентов, магистрантов, докторантов, представителей бизнеса, руководителей среднего и высшего звена, а также исследователей, интересующихся теорией и практикой современного менеджмента в Республике Казахстан.

УДК 005:378
ББК 65.290-2:74.58

ISBN 978-601-7166-12-0

Содержание

Белых Павел Александр
EMBA-O14-РАНХ
г.Алматы

Научный руководитель:
Куренкеева Г.Т., к.э.н.

Алматы
Менеджмент
Университет

Роль информационной безопасности в коммерческом банке

Коммерческие банки, являясь важнейшим финансовым институтом нашего общества, должны отвечать и следовать определенным правилам информационной безопасности с целью создания надежной системы безопасности как гаранта сохранности активов, привлечения клиентов, сохранности их персональных данных.

В настоящее время коммерческий банк превратился в IT компанию с лицензией на право управления финансами и проведения финансовых операций. Современный банк является цифровым и опирается на цифровую платформу. Информационные технологии широко и повсеместно используются банками. Практически любой современный универсальный казахстанский банк располагает в своем арсенале системами, позволяющими успешно вести бизнес, например, системами дистанционного банковского обслуживания, системами по построению взаимоотношений с клиентами (CRM), системами управленческой отчетности (MIS), служащих опорой руководству банка для поддержки и принятия управленческих решений, системами по построению и управлению бизнес процессами (BPM) [1, 2]. Каждая из перечисленных систем является довольно сложным высокотехнологичным продуктом, требующим особой квалификации для её эксплуатации и поддержки, в том числе и защиты. С конца 20 века технологии настолько трансформировали IT ландшафт банка (масштабная виртуализация IT - ресурсов, распространение мобильного доступа, переход к облачной I -инфраструктуре как на стороне самих банков, так и на стороне их клиентов), что заставляют участников банковского бизнеса использовать новые технологии и средства обеспечения информационной безопасности. Внедрение самых современных технологий в области IT требует использования таких же передовых технологий информационной безопасности.

Усиление банковской конкуренции, развитие банковских технологий, гибкая адаптивность применения IT привели к более широкой автоматизации услуг банка. Теперь банки фокусируют свое внимание не просто на платежах, а на всем процессе от начала и до конца. Основную ценность для современного казахстанского коммерческого банка представляет информация. Ежедневно оказывая свои услуги, генерируя и обрабатывая большое количество информации, банк получает доход. Учитывая это, можно отметить, что стоимость и значимость банковской информации сегодня многократно возросли, поскольку она может быть использована в преступных целях. Каждый казахстанский коммерческий банк обязан обеспечить безопасность хранимых и обрабатываемых им данных. Банковские информационные системы и базы данных содержат конфиденциальную информацию о клиентах банка, состояния их счетов и проведения различных финансовых операций.

Любая деятельность банка подвержена рискам, и использование информационных технологий не является исключением. Экономические и финансовые риски от использования IT непосредственно связаны с тем, насколько эффективно банк обеспечивает конфиденциальность, целостность и доступность информации. Что в свою очередь непосредственно зависит от мер и процедур контроля, применяемых с целью защиты и поддержания целостности конфиденциальной информации, прохождения аудиторских проверок. Также влияние оказывает конкуренция на банковском рынке, особенно в период кризиса, как правило, это вывод нового банковского продукта в минимально возможное время.

Особенности информационной безопасности банков.

Факторы, которые специфичны именно для банковского сектора, следующие.

1. Информация, которая хранится и обрабатывается банком - это реальные деньги. При открытом доступе к этой информации через компьютеры могут выдаваться кредиты, производиться выплаты, осуществляться перевод денег со счета без ведома владельца данного счета. Определенно ясно, что любое указанное манипулирование приведет к убыткам различной степени. Именно эта особенность увеличила число мошенников, которые покушаются на банки.

2. Информация, имеющая отношение к банковской сфере, касается большого числа людей и организаций, то есть клиентов. Банк должен обеспечить должный уровень конфиденциальности информации, поскольку каждый клиент вправе рассчитывать, что банк будет заботиться о его интересах, поскольку от этого напрямую зависят репутация и успешность самого банка.

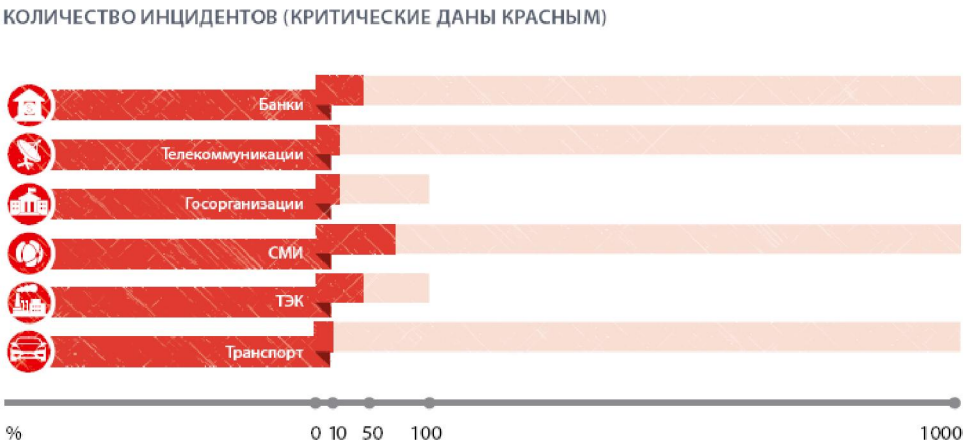
3. Банку необходимо быть конкурентоспособным, от этого напрямую зависит насколько удобно клиенту работать с его услугами, насколько они хороши, широк ли их спектр. Именно поэтому банк предоставляет возможность быстрого и неутомительного распоряжения денежными средствами своему клиенту. Легкость доступа к денежным активам увеличивает количество преступников, которые проявляют повышенный интерес к банковским системам.

4. Банк - это организация, работающая в режиме 24/7, с точки зрения ИТ. Он обязан обеспечить высокую надежность работы своих компьютерных систем даже в случаях нештатных ситуаций. Поскольку в отличие от большинства других компаний он несет ответственность не только за свои денежные средства, но и за деньги клиентов.

5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации [3].

По данным российской компании Pozitive Technologies, банки являются наиболее атакуемыми организациями (таблица 1). В Казахстане пока такой статистики не ведется.

Таблица 1. Количество инцидентов в коммерческих банках РФ за 2013 год.



Источник: Отчет «Инциденты в информационной безопасности крупных российских компаний за 2013 год». Компания Positive Technologies (4).

Информация компании «Лаборатория Касперского», занимающейся аналитикой в части информационной безопасности, свидетельствует о смещении фокуса атак на финансовые организации, они стали целевыми и высокопрофессиональными [5]. Ярким примером тому служит приведённая информация (рисунок 1) по группировке Carbanak (с одноименным названием зловредного программного обеспечения). Злоумышленники проникали в сеть банка-жертвы и искали критически важную систему, с помощью которой из атакованной финансовой организации выводили денежные средства. Украв у банка значительную сумму (от 2,5 до 10 млн долларов), преступники искали следующую жертву [5].

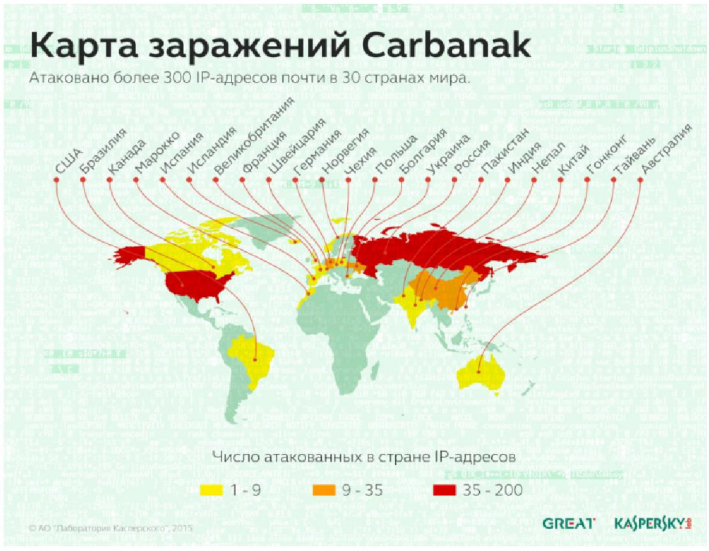


Рисунок 1 - Карта заражений трояном Carbanak

Заботясь о финансовом состоянии и репутации на рынке, банку необходимо выделять свои ресурсы для безопасности одной из основных своих ценностей – информации. В современных коммерческих банках для этого создаются структуры, задача которых обеспечение информационной безопасности. В Казахстане данное направление получило развитие сравнительно недавно, существует ряд нормативно-правовых актов регулятора, постановления Правления Национального Банка Республики Казахстан № 29 от 26 февраля 2014 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня», №80 от 31 марта 2001 года «Об утверждении Правил по обеспечению

безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций». (Последнее сейчас находится в переработке и по ней ведется обсуждение в банковском сообществе). В целом они соответствуют общему духу и направлениям, которые существуют в развитых странах. Существует Закон Республики Казахстан № 94-V «О персональных данных и их защите» от 21 мая 2013 года (с изменениями от 24.11.2015 г.). Настоящий Закон регулирует общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных.

Вместе с тем с существуют тенденции, на которые еще следует обратить внимание и которые не затронуты в указанных нормативно-правовых документах:

1. Применение банкоматов и платежных терминалов.

2. Применение пластиковых платежных карт (скорейший переход на карты, оснащенные микропроцессором, и запрет выпуска карт, им не оснащенных). Пластиковые карты с микропроцессором являются более технологически защищенными от несанкционированного воздействия в отличие от карт с магнитной полосой.

3. Требования к порядку разработки и распространения специализированного программного обеспечения, предназначенного для использования клиентом при переводе денежных средств.

4. Процедуры приостановления проведения платежей по переводу денежных средств в случае обнаружения признаков мошеннических действий.

5. Защиты сервисов, расположенных в сети Интернет, от внешних атак (DDOS-атак).

6. Зашита платежей предполагает обеспечение безопасности подтверждения клиентом платежа. Что решается использованием устройств защищенного хранения ключей электронной цифровой подписи (ЭЦП) и защищенной выработки этой подписи. А так же доверенных инструментов позволяющих безопасно использовать ЭЦП и мониторингом платежей на предмет выявления подозрительных или потенциально мошеннических сделок.

7. Обязательности соответствия казахстанских банков требованиям стандарта PCI DSS. В части безопасности платежных систем, признанным стандартом является payment Card Industry Data Security (PCI DSS). В него входят такие карточные системы, как Visa, Master Card, American Express, JCB. (Основной упор в стандарте делается на обеспечении безопасности сетевой инфраструктуры и защите хранимых данных о держателях платежных карт). Сертификация казахстанских банков по указанному стандарту идет довольно медленно, и отечественного аналога ему на сегодняшний момент нет.

Если банки смогут обеспечить требуемый высокий уровень информационной безопасности, это позволит свести к минимуму следующие риски [6]:

- Риск потери, а также разрушения ценных данных;
- Риск утечки информации, которая составляет служебную/коммерческую/банковскую тайну;
- Риск распространения во внешней среде информации, которая будет угрожать репутации банка;
- Риск использования неполной или искаженной информации в деятельности банка.

Все перечисленные риски имеют общую характеристику, их реализация влияет финансово на организацию.

Таким образом, мы видим, как и насколько серьезно в цифровую эпоху стала важной и актуальной задачей обеспечения информационной безопасности банка, и насколько легко банковская информация может подвергнуться зловредным манипуляциям. Их влияние выражается, как правило, в виде финансовых величин:

1. Затрат на обеспечение информационной безопасности;

2. Ущерба/Затрат на покрытие ущерба, возникшего в результате отсутствия либо слабой информационной безопасности.

Банк не может заниматься основной деятельность без обеспечения определенного уровня защиты информации, который требует определённых инвестиций и внимания, и именно эти инвестиции делают его более конкурентоспособным.

Источники:

1. Голенда Л.К., Громов В.И. Информационные технологии банка. Минск: «Издательство Гревцова», 2013
2. Амириди Ю.В, Ашкинадзе А.В., Варов К.А. Банковские информационные системы: внутренний и внешний аспекты. М., 2010
3. Журавлев В.В., Целых А.Н. Особенности информационной безопасности банковских систем и меры по ее обеспечению. http://www.gramota.net/materials/1/2015/9/17.html
4. Отчет « Инциденты в информационной безопасности крупных российских компаний за 2013 год». Компания Positive Technologies. http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf)
5. Отчет компании «Лаборатория Касперского» https://securelist.ru/analysis/ksb/27519/kaspersky-security-bulletin-2015-evolyuciya-ugroz-informacionnoj-bezopasnosti-v-biznes-srede/
6. Астахов А. Искусство управления информационными рисками. М.: «ДМК Пресс», 2010.