Менеджмент рисков информационной безопасности

Определение

- Риск – это вероятность возможной нежелательной потери чего-либо при плохом стечении обстоятельств
- Риск информационной безопасности - вероятность возникновения ущерба вследствие нарушения целостности, конфиденциальности и доступности информационных активов

Описание риска

Примеры

Источник угрозы	Использует уязвимость	Возникает угроза
Вирус	Отсутствие антивирусного программного обеспечения	Заражение вирусом
Хакер	Уязвимости в коде Отсутствие системы обнаружения вторжений	Несанкционированный доступ к конфиденциальной информации
Пользователи	Неверно настроенный параметр операционной системы	Неисправность системы
Пожар	Отсутствие огнетушителей Отсутствие плана действий при пожаре	Здание и оборудование повреждены, возможны человеческие жертвы
Сотрудник	Отсутствие требований и обучения Отсутствие контроля	Доступ к критичной информации Внесение изменений в вводимую информацию
Подрядчик	Слабая система контроля доступа	Утечка конфиденциальной информации

Менеджмент риска

№	Этапы	Действия
1	Планирование	Определение области оценки риска и IRM-группы
2	Анализ и оценка рисков	идентификация и оценка активов идентификация угроз идентификация уязвимостей анализ защитных мер прогнозирование последствий оценка вероятности реализации угрозы измерение уровня риска
3	Обработка рисков	Выбор варианта реагирования на риски: - уход от риска - минимизация риска - перенос риска - принятие риска
4	Реализация плана обработки риска	Проведение мероприятий, направленных на управление рисками (внедрение защитных мер, отказ от деятельности, страхование риска, проведение обучения по повышению осведомленности персонала и партнеров организации во вопросам ИБ и т.д.)
5	Контроль и мониторинг	Регулярная оценка риска и отслеживание влияющих на него факторов

Оценка риска

УЩЕРБ → ЧАСТОТА ↓	Незначительный <50 000 KZT	Малый 50 000–1 000 000 KZT	Средний 1 000 000–10 000 000 KZT	Существенный >10 000 000 KZT
Маловероятно (реже 1 раз/год)	Низкий	Низкий	Низкий	Умеренный
Редко (1 раз /год)	Низкий	Низкий	Умеренный	Высокий
Иногда (2-3 раза/год)	Низкий	Умеренный	Умеренный	Высокий
Часто (6-12 раза/год)	Умеренный	Умеренный	Высокий	Критичный
Очень часто (чаще 1 раза/мес)	Умеренный	Высокий	Высокий	Критичный

Задача

- В банке «АВС» обслуживается 20 тысяч клиентов, 40% из которых составляют держатели депозитов, остальные пользуются только кредитными продуктами банка. За последние два года на маркетинговые акции было потрачено порядка десяти миллионов тенге. С целью упрощения обслуживания для своих клиентов банк заказал разработку интернет-сайта, который будет запущен на следующей неделе. Планируется, что благодаря услугам, которые будут доступны клиентам через систему ДБО, доходность банка будет составлять порядка тридцати миллионов тенге в месяц. В SLA с компанией, предоставляющей техническую поддержку сайта прописано, что время восстановления при недоступности его сайта составляет 2 часа после обращения.
- Какие угрозы возникают в связи с запуском нового продукта?
- Проанализировать и оценить один риск

Методики

- **ISO 27005**
- ***NIST SP 800-30*** и ***800-66***
- ***FRAP*** (Facilitated Risk Analysis Process)
- ***OCTAVE*** (Operationally Critical Threat, Asset, and Vulnerability Evaluation
- ***FAIR*** (Factor Analysis of Information Risk)
- ***AS/NZS 43 60***
- ***CRAMM*** (CCTA Risk Analysis and Management Method)
- ***Spanning Tree Analysis***
- ***ENISA***
- ***Harmonized Threat and Risk Assessment Methodology***
- ***РС БР ИББС-2.2***

Каталоги угроз

- *BSI – Threats Catalogue Force majeure*
- *MAGERIT: Risk Analysis and Management Methodology for Information Systems*
- *IT-Grundschutz catalogues*
- *ISO 13335-3-2007*
- *ISO 27005*
- *БДУ ФСТЭК России*


Спасибо за внимание!