Компания «РНТ»
Российские наукоемкие технологии

О повышении киберустойчивости информационных систем кредитных организаций

Андрей Курило,
главный советник, компания «РНТ»
КТН,
доцент финансового университета
при Правительстве РФ

О компании

Компания «РНТ»

Компания «РНТ»
(АО «РНТ», год образования 1993)

Ведущий российский системный интегратор, разработчик автоматизированных информационных и телекоммуникационных систем в защищенном исполнении, сертифицированных ПЭВМ, изделий и программного обеспечения

Компания специализируется на создании концепций и комплексных решений в области инфо-телекоммуникационных и аналитических систем, средств и систем защиты и управления безопасностью

Гарантией качества является более чем 20-летний опыт компании, профессионализм специалистов, среди которых 150 квалифицированных инженеров, 36 кандидатов и 4 доктора наук.

Общие направления деятельности

Проектирование и внедрение автоматизированных информационных систем в защищенном исполнении, систем управления безопасностью, и др;

Производство средств, систем и программных Продуктов в защищенном исполнении;

Аудит и консалтинг информационной безопасности;

Исследования и оценка защищенности объектов;

Аттестация объектов информатизации по требованиям безопасности информации;

Услуги в области защиты персональных данных;

Техническое сопровождение оборудования и ПО, компьютерных систем, техническая поддержка, гарантийное и послегарантийное обслуживание продукции компании;

Обучение;

Работы в области импортозамещения.

Факторы, трансформирующие ландшафт угроз информационной безопасности

Компания «РНТ»
Российские наукоемкие технологии

1. Резкое усиление активности многих государств в области «кибервойн», прежде всего атак на «чужие» ресурсы, массовое создание специальных подразделений (кибервойск), разработка специальных средств и методов ведения операций в информационном пространстве.

   В отличие от физического мира, государственная граница в информационном пространстве проходит не по установленной и согласованной на международном уровне линии разграничения, а в лучшем случае, по периметру защиты информационной системы. В худшем случае, ее вообще нет.

1. Появление новых видов атак, характеризующихся:
   - новыми версиями ВК, как правило, не обнаруживаемыми стандартными средствами;
   - «универсальным» способом инфицирования (наиболее простой, самый распространенный и и по- прежнему эффективный - через почтовые отправления);
   - расширением целей атак, реализуемых ВК уже внутри системы;
   - скрытностью работы ВК.

3. Постепенное снижение эффективности антивирусных средств.
4. По-прежнему высокая зависимость отечественных информационных систем от импортных технических и программных средств, актуализация вопросов, связанных с недекларируемыми возможностями зарубежного программного обеспечения и оборудования, рост вероятности использования этих инструментов.
5. Рост квалификации внутреннего и внешнего нарушителя.

Результат, наблюдаемый в финансовых системах *–объективный тренд снижения реального уровня защищенности информационных систем, более высокий риск заражения новыми видами ВК, появление инцидентов, связанных с результативными атаками на денежные средства КО, аккумулированных на их корреспондентских счетах.*

Киберустойчивость: что это такое?

Компания «РНТ»
Российские наукоемкие технологии

Киберустойчивость - способность информационной системы сохранять свою функциональность и предоставлять пользователю заранее оговоренные сервисы в условиях воздействия на нее актуальных для этой системы атак, идентифицированных в соответствующей модели угроз и модели нарушителя.

Обеспечение киберустойчивости предполагает:

1. Надежное отражение известных атак силами и средствами системы обеспечения информационной безопасности системы.
2. Контроль за использованием учетных записей.
3. Способность быстро обнаружить и идентифицировать инциденты, возникшие в результате реализации атаки на защищаемую систему.
4. Способность быстро принять меры по купированию инцидента и устранению его последствий.
5. Возврат системы в исходное, заведомо «нормальное» состояние, предшествовавшее кибератаке.

1. Надежное отражение известных атак

Компания «РНТ»
Российские наукоемкие технологии

Факторы успеха.

1. Наличие официальных, обязательных, ясных, понятных и непротиворечивых требований по безопасности.
2. Реализация систем защиты в соответствии с требованиями и принятыми для них моделей угроз и нарушителей.
3. Использование в необходимых случаях программных и технических средств, имеющие соответствующие сертификаты соответствия.
4. Усиление контроля за использованием и менеджментом учетных записей.
5. Организация системы менеджмента информационной безопасности.
6. Обученный и подготовленный персонал.
7. Наличие системы внутреннего контроля.
8. Эффективный внешний независимый контроль (аудит) выполнения требований.
9. Для малых организаций – надежный аутсорсинг безопасности, возможно с использованием страхования рисков инцидентов информационной безопасности.

2. Быстрое обнаружение и идентификация результативных атак, классифицируемых как инцидент

Компания «РНТ»
Российские наукоемкие технологии

Факторы успеха.

1. Наличие требований по безопасности, предусматривающих необходимость использования систем защиты класса СОА.
2. Внедрение и практическое использование СОА, выявляющих и блокирующих активность попавшего вовнутрь защищаемой среды вредоносного кода, необнаруживаемого средствами антивирусной защиты, путем анализа сетевого трафика и поведенческих сигнатур непосредственно на атакуемых АРМах и серверах.
3. Фильтрация сетевого трафика. Использование МСЭ прикладного уровня.
4. Организация системы менеджмента СОА.
5. Контроль за использованием учетных записей.
6. Наличие обученного и подготовленного персонала.
7. Наличие системы внутреннего контроля.
8. Эффективный внешний контроль (аудит) выполнения требований.
9. Для малых организаций - надежный аутсорсинг безопасности и не только безопасности (Стандартизованная обработка данных в виртуальной среде. Облачное хранение данных), возможно с использованием страхования рисков инцидентов информационной безопасности.

3. Быстрая локализация и ликвидация последствий атаки.

Компания «РНТ»
Российские наукоемкие технологии

Факторы успеха

1. Наличие системы менеджмента инцидентов, в которую включен контур СОА. Готовность и способность системы быстро распознать, классифицировать и купировать атаку, не дать развиться инциденту.
2. Наличия плана действий в чрезвычайных обстоятельствах.
3. Наличие специалистов, наделенных функциональными полномочиями принятия решения на основе анализа данных СОА и иных систем, о факте инцидента, его идентификации, парированию, устранению ущерба, восстановлению систем сначала в работоспособное, а потом в исходное состояние.
4. Обученный и подготовленный персонал.
5. Наличие системы внутреннего контроля.
6. Эффективный внешний контроль (аудит) выполнения требований.

4. Возврат системы в исходное состояние.

Компания «РНТ»
Российские наукоемкие технологии

Факторы успеха

1. Наличие плана действий по возвращению системы сначала в работоспособное, а потом в исходное состояние.
2. Наличие необходимых работоспособных, заведомо «чистых» резервных систем, эталонных копий ПО и данных.
3. Обученный и подготовленный персонал.
4. Наличие системы внутреннего контроля.
5. Эффективный внешний контроль (аудит).

Общие факторы

Компания «РНТ»
Российские наукоемкие технологии

- Наличие требований по безопасности, оформленных и введенным в действие соответствующим образом
- Наличие эффективных средств защиты, прежде всего, СОА с перспективой ее подключения к СОПКА в соответствии с готовящемся ФЗ «О защите объектов критической инфраструктуры»
- Обученность персонала
- Включение в систему менеджмента процессов, обеспечивающих киберустойчивость организации, включая ее восстановление после успешных атак
- Эффективный внешний контроль (аудит)
- Эффективный и надежный аутсорсинг
- Доверие со стороны регулятора к организациям, предоставляющим услуги аудита и аутсорсинга

Вопросы, требующие решения

Компания «РНТ»
Российские наукоемкие технологии

Как сделать все это эффективным?

Как реализовать эффективный аутсорсинг?

Как организовать эффективный контроль, в том числе и за аутсорсерами?

Как добиться доверия со стороны регулятора?

СПАСИБО ЗА ВНИМАНИЕ!

Андрей П. Курило
АО РНТ, главный советник,
КТН,
доцент Финансового Университета
при Правительстве РФ