Кризис? Осмотреться в отсеках!

Однажды наступил кризис и нам сказали: Денег выделять будем только на самое важное, или не будем, повышайте эффективность уже имеющихся систем защиты!

Писать про то, как себя вести в кризис Вендорам, Интеграторам, Поставщикам и другим жителям нашей отрасли? Да они сами лучше меня знают… Поговорим про Заказчиков, да что там, расскажу про себя.

Я выработал некоторые координаты для систем, связанных с ИБ. Вот эти координаты:

В общем случае служба информационной безопасности должна обеспечивать деятельность в интересах бизнеса компании по следующим направлениям:

Знать. Контролировать. Защищать. Влиять.

1. Знать.

Информационные активы компании; ИТ-инфраструктуру компании; Владельцев информационных активов; Потребителей информационных активов; Порядок хранения, передачи, обработки данных; Требования, предъявляемые правовыми и нормативными актами; Бизнес-процессы, связанные с обработкой информационных активов; Планы развития или реорганизации ИТ-инфраструктуры и связанных процессов; Источники угроз безопасности информации и т.п.

2. Контролировать.

Состояние защищенности информационных активов; Изменения: в ИТ-инфраструктуре компании; в информационных активах компании; в перечне субъектов доступа; в информационных потоках; в правилах разграничения доступа; в бизнес-процессах, связанных с ИТ-инфраструктурой; в нормативных и правовых актах и т.п.

Порядок разграничения доступа к информационным активам; Исполнение политик информационной безопасности; Источники угроз безопасности информации и т.п.

3. Защищать.

Информационные активы компании; ИТ-инфраструктуру компании включая:

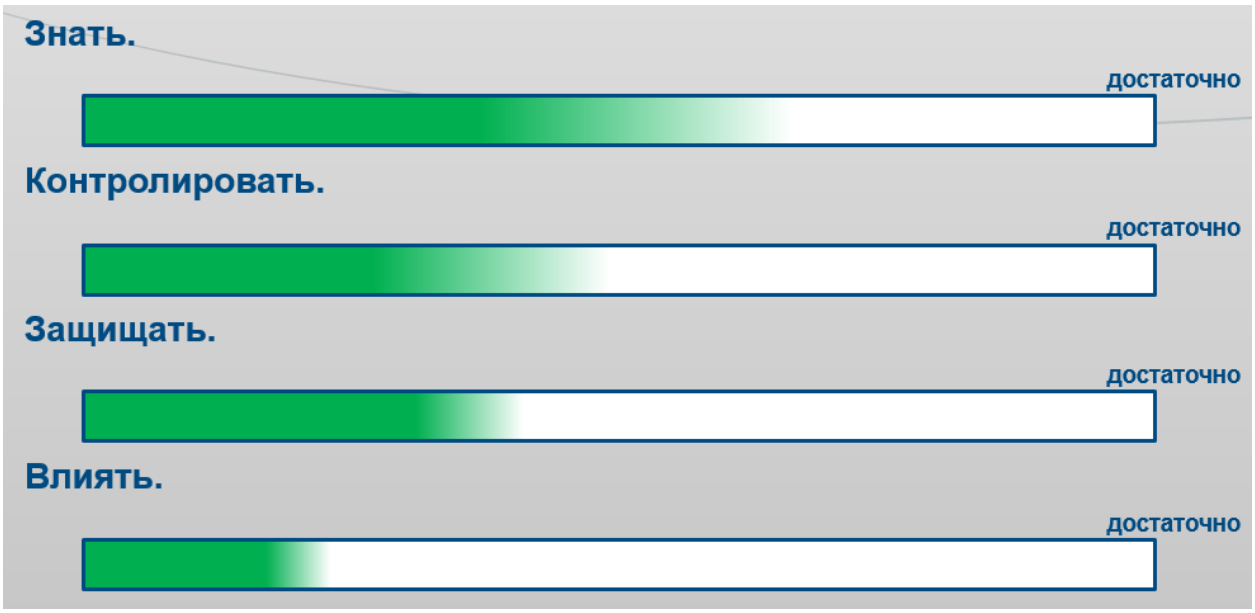
средства вычислительной техники; средства связи и каналы связи (сетевую инфраструктуру); СХД; Мобильные и носимые устройства.

Персональные данные; Информационные активы партнеров; Информацию, влияющую на репутацию компании и т.п.

4. Влиять.

На: планы развития ИТ-инфраструктуры компании; порядок обработки информационных активов; порядок разграничения доступа к информационным активам; Формирование и исполнение политик обработки информации; Выработку решений, затрагивающих ИТ-инфраструктуру компании. На источники угроз безопасности информации.

Как может выглядеть состояние по каждому направлению:



Очевидно, что очередность идет от Знаний к Контролю и только потом к Защите и Влиянию. Каждый уровень опирается на предыдущий. И тут

важнейшими являются Знания и Контроль, или как говорят в нашей среде «глазастость»! Да, можете нарисовать себе подобное и расставить метки по каждому направлению. Полезно составить перечень того что нужно сделать для того чтобы повысить «глазастость» и что этому мешает.

Теперь обратимся к следующим координатам:

Дело в том, что системы, помогающие обеспечить указанные выше 4 направления, тоже можно поделить на 4 класса по степени первоочередности и влиянию на все аспекты безопасности. Вы можете сами составить свою картину, но моя такая:

1. Системы, обеспечивающие базовые «Знание, Контроль, Защиту» (ЗКЗ) на периметре. (межсетевые экраны, WSA, ESA, анти-спам, антивирусы на периметре и т.п.)
2. Системы, обеспечивающие базовые ЗКЗ внутри периметра. (AD, антивирусы, бекапы, встроенные механизмы и т.п.)
3. Системы, обеспечивающие ЗКЗ на прикладном уровне (DLP, IPS, SIEM, IDS и т.п.)
4. Системы поддержки типа автоматизации менеджмента рисков, отчетности и т.п.

Тут важно понимать, очередность тоже идет от 1 к 4 уровню.

Системы 1 класса как правило уже есть. Эти системы очевидны, задачи по их применению понятны и тут сильно не разгуляешься. Закупили – внедрили – поддержка. Системы 2 уровня или встроенные, или стараются применять «бесплатные» версии или аналоги на свою голову.

В кризисные времена системы 3 уровня восходят на трон! Они начинают превращаться в нечто особенное и вот почему:

Из-за того, что они обладают некоторыми свойствами привыкания пользователей к ним и в условиях, когда Заказчик не готов за них платить можно использовать это свойство, внедряя такие системы в режиме «продолжительный пилот». Когда Заказчик будет готов вкладывать в ИБ – куда нести деньги становится очевидным!

Очевидно применение средств, повышающих «глазастость» и тут нет альтернативы DLP системам. Прежде всего отечественным! Хотя бы потому что они гибче и возможность прямого общения с разработчиком – огромный плюс. Вообще нужно отметить, что месяц применения DLP продуктов компании INFOWATCH окупает ее стоимость полностью! При этом, система позволяет использовать ее не только по «прямому назначению». Известны примеры, когда продукты INFOWATCH использовались как некий специализированный SIEM и с его помощью, за счет автоматизированного анализа активностей в сети были выявлены и APT атаки и несколько уникальных BOTNET активностей которые не удавалось выявить другими специализированными средствами, что делает их систему уникальным средством с широкими возможностями. Так же системы INFOWATCH позволяют работать с данными косвенно демонстрирующими активность использования ресурсов и тут уж насколько хватит смекалки ее пользователям для работы. Это еще раз подтверждает, что грамотно сделанный продукт в грамотных руках специалиста это сила!

Именно на повышение уровня Знаний и широких возможностей Контроля в кризисное время – делают особенным применение продуктов 3 класса.

Итак, если случился кризис и бюджеты ограничены: внедряйте DLP систему. Если вы еще последуете моему совету и выберете продукты компании INFOWATCH – у вас будет целый набор скрытых дополнительных возможностей в части их не стандартного применения! Гарантирую, это даст максимальный эффект и окупится в течении месяца!

И запомните: знать и контролировать – вот функции, важность которых в кризис возрастает кратно!