Центр мониторинга – предупреждение атак и контроль обеспечения информационной безопасности

Васильев А.Л.
ЗАО «Перспективный Мониторинг»

В условиях информационного обмена, каждая организация и пользователь подключаясь к информационным сетям могут быть подвержены компьютерным атакам. Установка обновлений средств антивирусной защиты в более, чем в половине из всех случаев фактов компьютерных атак не уберегли жертву от компьютерных атак, так как используемые злоумышленниками слабости программного обеспечения и техники остаются не заметны. В 2016 году отмечен двукратный рост компьютерных атак по сравнению с предыдущим годом, в среднем каждую неделю осуществляется до двух атак направленных на организацию.

Сложившаяся ситуация вокруг компьютерных атак, проводимых с целью нарушения функционирования информационных систем актуальна не только для финансовых институтов, но предприятий и госучреждений, убытки в годовом исчислении измеряются десятками миллиардов рублей.

Среднее время затраченное на восстановление инфраструктуры организации после успешно проведенной атаки оценивается в 46 дней, аналитики оценивают потери в размере около 1 200 000 рублей.

Специализированными Центрами мониторинга осуществляется оперативное выявление угроз и инцидентов, связанных с компьютерными атаками, проводится постоянное исследование информационных систем на основе анализа событий информационной безопасности, регистрируемых средствами обнаружения вторжений и другими источниками в сети.

Каждое событие информационной безопасности идентифицируется и означает определённое состояние системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности (несанкционированное подключение, использование не разрешенных или уязвимых программ) или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности. Эксперты Центра мониторинга анализируют ситуацию и принимают решение о применении необходимых мер.

При этом не каждое события становится инцидентом, учитывается появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми может быть связана высокая

вероятность компрометации бизнес операций и создание угрозы системе информационной безопасности.

Источниками событий информационной безопасности, анализируемые экспертами могут быть сетевые и узловые системы обнаружения вторжения, сетевые устройства, сканеры защищённости, антивирусные решения и специализированные системы перехвата атак, а также другие системы.

При обработке событий и инцидентов информационной безопасности аналитики Центра мониторинга приоритезируют и классифицируют инциденты в зависимости от подверженных воздействию ресурсов:

- Инциденты высокой критичности. Инциденты информационной безопасности, связанные с критической информационной инфраструктурой - ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).

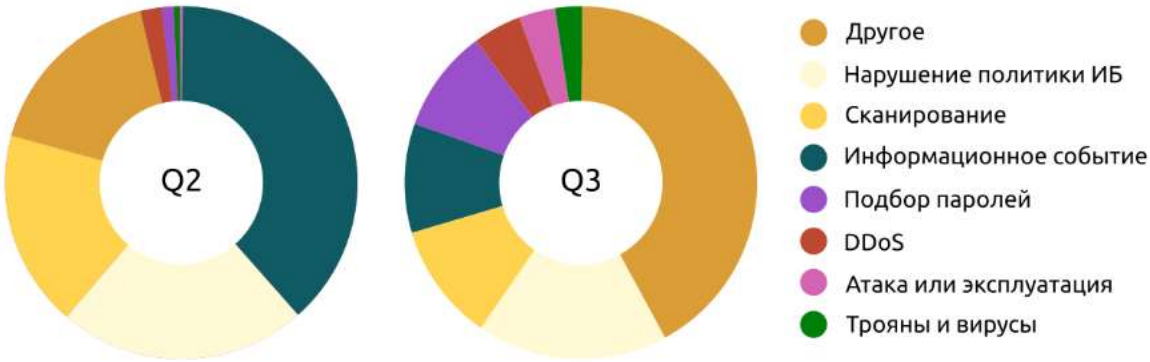
- Инциденты средней критичности Инциденты, связанные с некритичными ресурсами Серверного сегмента.

- Инциденты низкой критичности. Инциденты, связанные с некритичными ресурсами Пользовательского сегмента.

Аналитики Центра мониторинга могут определить высокую критичность инцидента, если посчитают, что инцидент может привести к серьёзным негативным последствиям.

К примеру, за квартал сотрудники Центра мониторинга исследуют информационные системы разных организаций с количеством подключённых узлов более 1500 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.). Только сенсоры системы обнаружения вторжений фиксируют более 25 000 000 событий информационной безопасности, анализ которых позволил выявить 21 инцидент, связанный с компьютерными атаками.

Сравнение классов проанализированных Центром мониторинга событий во 2 и 3 квартале 2016 года



Распределение событий показывает, что

«Информационное событие» — события, несущие информационную направленность, которые могут быть полезны при разборе инцидента.

«Нарушение политики ИБ» — события, свидетельствующие о действиях, предположительно нарушающих требования Политики ИБ контролируемой организации.

«Атака или эксплуатация» — события, свидетельствующие о попытках удалённого исполнения кода или эксплуатации уязвимостей на контролируемых ресурсах.

«Сканирование» — события, свидетельствующие об исследовании сети перед попыткой атаки.

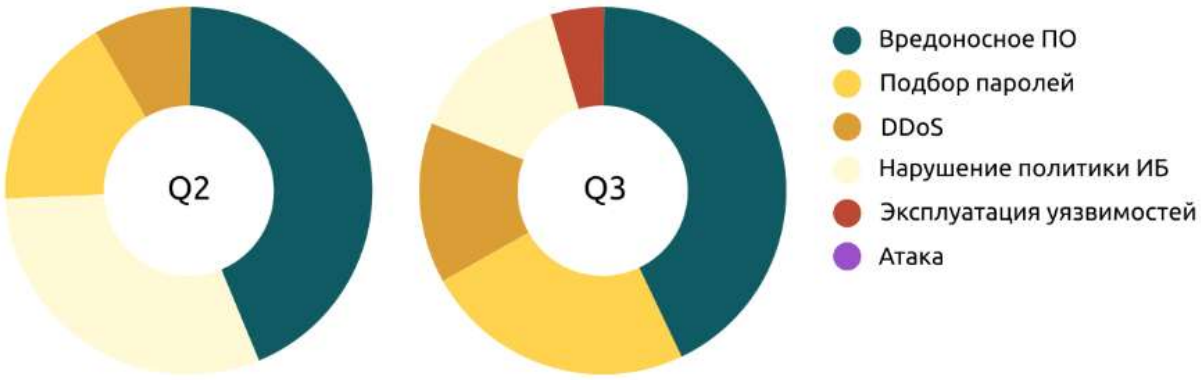
«Подбор паролей» — события, свидетельствующие о попытках получения доступа к контролируемым ресурсам путём подбора аутентификационных данных.

«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«DDoS» — события, свидетельствующие о попытках осуществления распределённых атак на отказ в обслуживании.

«Другое» — события которые по своей сути не могут быть отнесены к одному из вышеперечисленных классов.

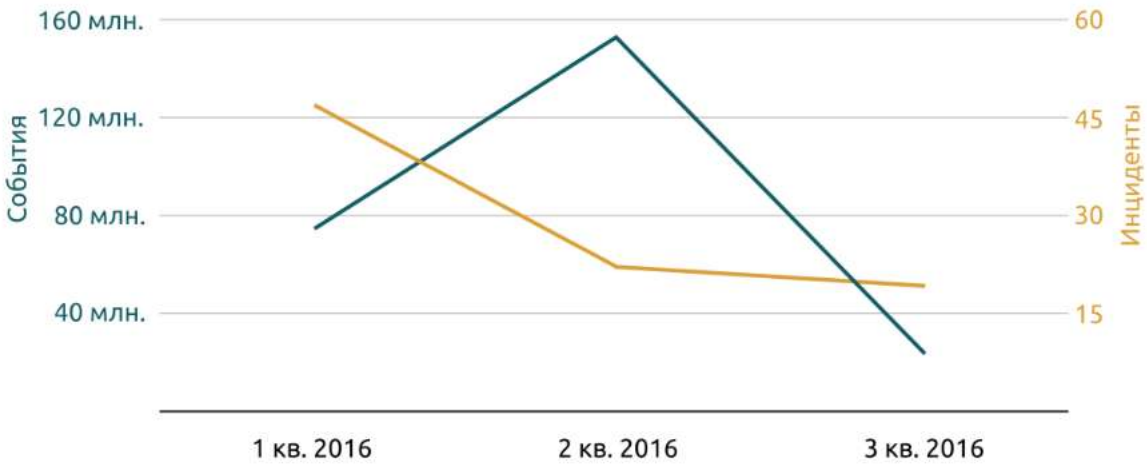
Сравнение типов выявленных инцидентов Центром мониторинга во 2 и 3 кварталах 2016 года



Наиболее актуальными и критичными из выявленных инцидентов являются атаки, связанные с попытками получения несанкционированного доступа к ресурсам организаций.

Несвоевременность реагирования на выявленные инциденты может привести к серьезным финансовым и репутационным потерям. Так за 2016 год ущерб от компьютерных атак оценен в более чем в 70 миллиардов рублей.

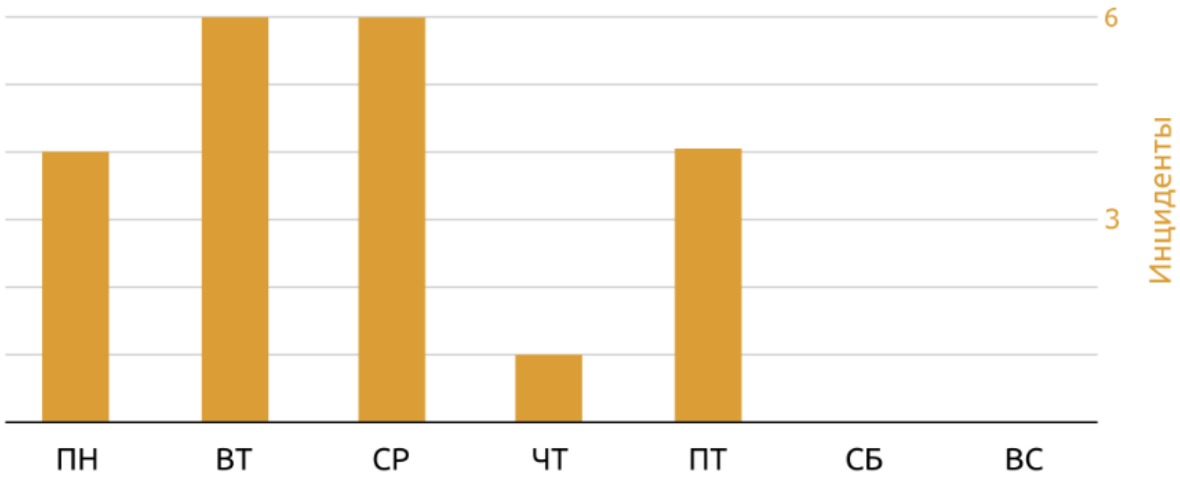
Распределение событий и инцидентов обработанных Центром мониторинга в 2016 году



Количественные изменения отношения зарегистрированных событий и выявленных инцидентов, связанно с разработкой специалистами Центра мониторинга новых правил для выявления паттернов компьютерных атак в сетевом трафике для системы обнаружения вторжений.

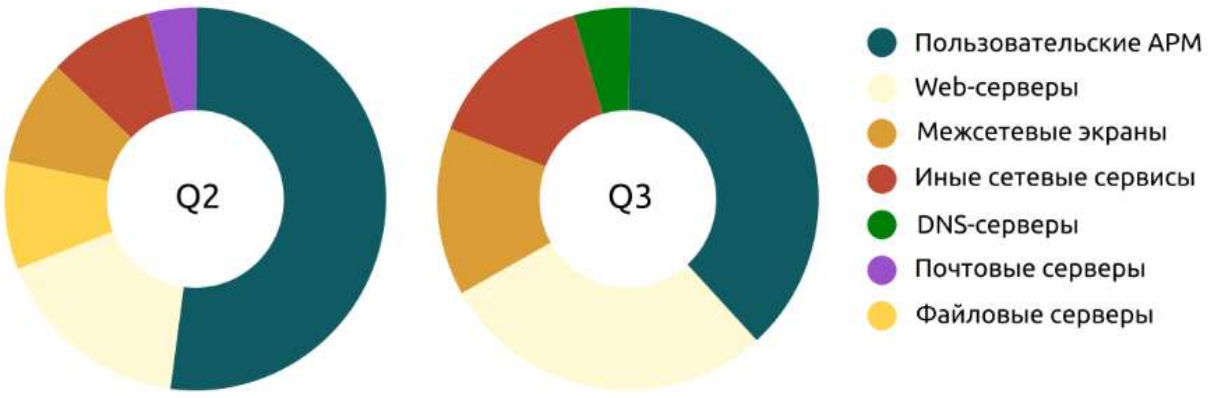
Разработка новых правил позволила быстрее выявлять инциденты и учитывать новые техники используемые атакующими, в том числе при DDOS атаках, реагировать на проявление признаков на ранних стадиях, тем самым снижая возможные негативные последствия компьютерных атак.

Распределение инцидентов выявленных Центром мониторинга по дням недели



Фиксация большей части инцидентов в середине недели, связанно с активностью пользователей в этот период, большинство пользователей становятся жертвами в связи с неосведомленностью или не внимательностью, при получении фишинговых писем, содержащих с виду, безобидный контент с вредоносным вложением или при обращении к модифицированным злоумышленниками Интернет ресурсам, содержащих вредоносный код.

Информационные ресурсы подверженные атакам во 2 и 3 квартале 2016 года



Наиболее часто воздействие злоумышленниками оказывается на Web – ресурсы организаций и пользовательский сегмент, но в целом угрозе эксплуатации уязвимостей подвержены все сегменты взаимодействующие в информационной сети.

Необходимость принятия организационных и технических мер по предупреждению и выявлению инцидентов, связанных с компьютерными атаками нашло отражение не только в Федеральном законе № 149, но и в требованиях ФСТЭК России, приказы №17,21 и 31, а также в Указе Президента Российской Федерации №31с.

Привлечение специализированных Центров мониторинга владельцами и операторами информационных систем, позволяет быстро интегрировать решения Центра мониторинга в инфраструктуру без необходимости ее изменения, повысить качество и скорость реагирования на инциденты, уменьшить время на поиск причин, решить проблему с ресурсами, получить экспертизу по анализу состоянию информационной сети, в том числе контролировать:

- Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- Своевременное обнаружение фактов несанкционированного доступа к информации;
- Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- Предотвращение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- Предупреждение возможности попытки модификации или уничтожения информации вследствие несанкционированного доступа к ней;
- Обеспечение уровня защищенности информации;
- Реагирование на появление новых угроз.

На ряду с техническими преимуществами при привлечении специализированных Центров мониторинга, владельцы и операторы информационных систем получают выгоды от уменьшения финансовых рисков, уменьшении репутационных рисков, уменьшения затрат на восстановление систем, возможность реинвестировать сэкономленные средства от потерь.