Маркетинг - изменения, последние тренды

Что мы покупаем?

Маркетинг - изменения, последние тренды

- Изменение отношения к информационной безопасности от «Зачем?» до …
- Угрозы это двигатель прогресса в ИБ
- Этапы покупки решения по ИБ со стороны покупателя:

1) Определяем потребность. Анализирум угрозы и уязвимости которые мы обнаружили в процессе эксплуатации нашей системы или систем.

2) Определяем решения, которые существуют на рынке.

3) Производим выбор поставщиков решения.

4) Проводим пилотный проект в некой тестовой среде или в некой "песочнице" являющейся частью "живой" инфраструктуры компании.

5) Проводим сравнение результатов пилотного тестирования, если у нас было несколько продуктов.

6) Проводим окончательный выбор поставщика/решения.

7) Заключаем контракт/договор на поставку и внедрение.

8) Внедрение системы.

9) Эксплуатация системы.

- Этапы покупки решения по ИБ со стороны продавца:

Маркетинг - изменения, последние тренды

- Тренды угроз

SANS 2017 имеем следующую статистику по основным угрозам: **1. Фишнг** **2. Вымогатели** **3. DDoS** **4. APT атаки** **5. Повышение привилегий** **6. Трояны** **7. Вредоносные программы** **8. SQL injection, cross-site scripting or other web app attacks** **9. Смешанные/комбинированные атаки Blended threats** **10. Программы-шпионы** **11. Средства удаленного администрирования** **12. Мобильные вредоносны** **13. MITM атаки** **14. Связанные уязвимости Chained exploits** **15. Кейлоггеры** **16. Черви** **17. Вредонос с изменяемым кодом Polymorphic malware** **18. Уязвимости уровня ядра Kernel-mode exploits**	**статистика SANS за 16 год:** **1. Фишинг** **2. Направленный фишинг** **3. Трояны** **4. Вымогатели** **5. Шпионское ПО (программы слежения)** **6. DDoS** **7. SQL injection, cross-site scripting or other web app attack** **8. Черви** **9. Advanced persistent threat (APT)** **10. Мобильные вредоносны** **11. Повышение привилегий** **12. Кейлоггеры** **13. MITM атаки**

Маркетинг - изменения, последние тренды

- Тренды средств защиты

Gartner, считают, что к «горячим» ИБ-технологиям сегодня (ключевое слово — сегодня) можно отнести следующую четверку:

1) анализ сетевого трафика (NTA или NBAD);

2) обнаружение и реагирование на угрозы на рабочих местах (EDR);

3) анализ поведения пользователей (UEBA);

4) облачные брокеры/посредники безопасности (CASB).

Маркетинг - изменения, последние тренды

А что может пойти не так?

Что мы покупаем?