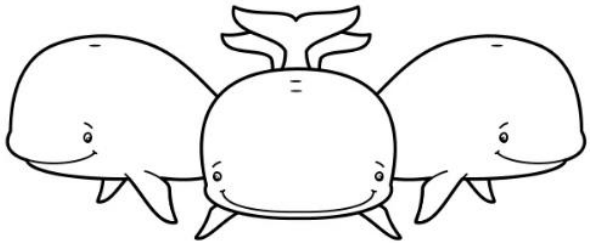
Центральный
научно-исследовательский
институт связи

Межоператорский центр анализа и мониторинга трафика веб-ресурсов на базе инфраструктуры ФГУП ЦНИИС

CIA

CIA – стандартная модель безопасности



— **конфиденциальности**, — означающего, что получить информацию могут только те субъекты ИС, которые имеют на это право;
— **целостности**, — означающего, что информация не была подвержена несанкционированной модификации;
— **доступности**, — означающего, что каждый субъект ИС, имеющий право на доступ к информации, имеет возможность реализовать его.

DDoS

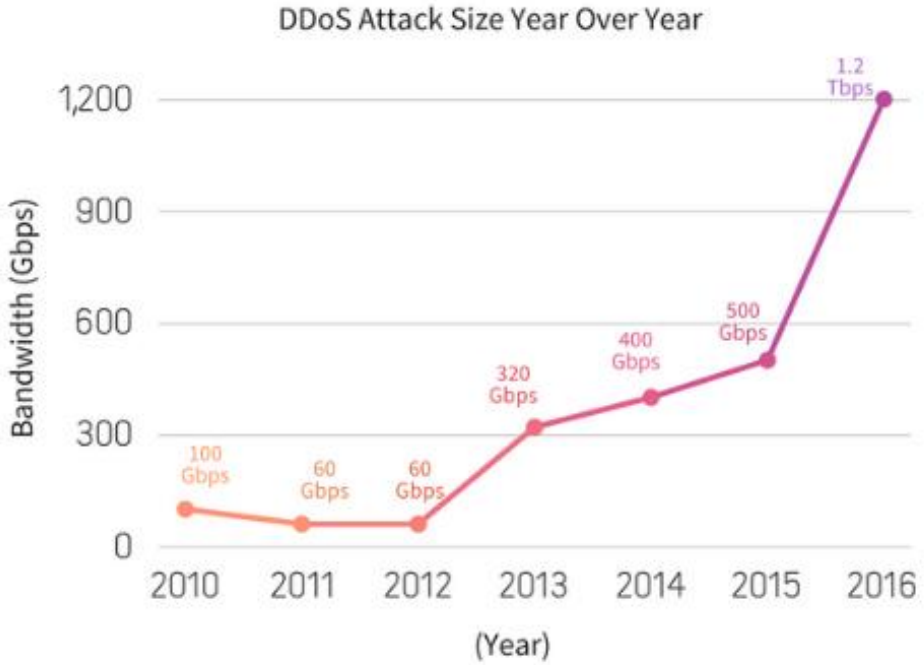
Distributed Denial of Service

распределённый отказ в обслуживании
«Распределённый» означает, что атака ведётся с большого числа компьютеров и других устройств, имеющих доступ в Сеть

DDoS

История

первые атаки —
1999-2000 гг.
на сервера FBI



Причины DDoS

Причины возникновения DDoS :

- конкуренция
- ограничение доступа к информации
- месть
- вымогательство
- развлечение
- политика

Истинные цели DDoS атаки

Часто под DDoS атаками маскируется основная задача - нарушение целостности и конфиденциальности ИС

Последствия такой атаки куда более ущербные, чем просто отказ в обслуживании клиентов, доля таких атак превышает 40% от общего числа атак

DDoS

- Каждый 3-4 сайт содержит всем известные уязвимости

- Значительное снижение стоимости DDoS атаки, рост бот-нетов, снижение технического порога для хакеров, экспоненциальный рост мощности и разнообразия атак из года в год

Центральный научно-исследовательский институт связи

События-триггеры DDoS атак в 2018г.

Крупные бизнес, спортивные и политические мероприятия

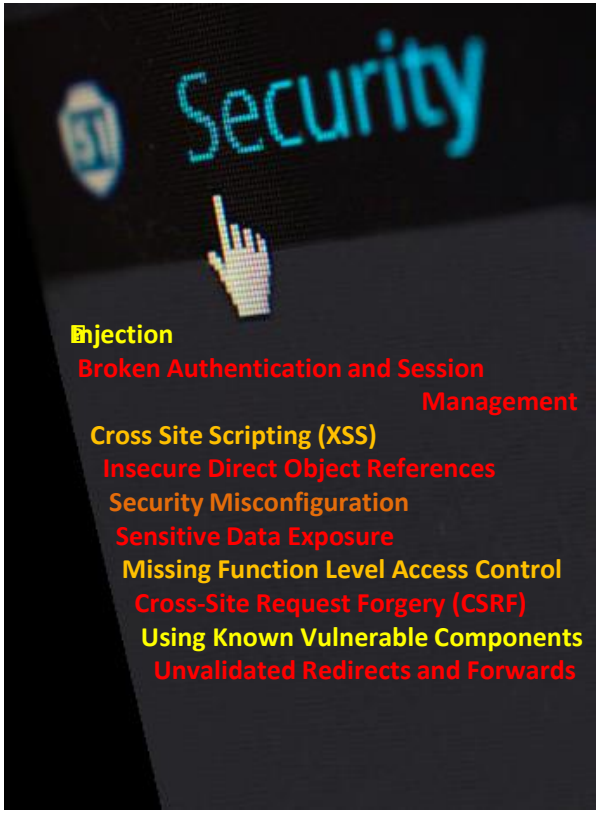
Выборы 2018

ЧМ по футболу

ПМЭФ 2018

Центральный научно-исследовательский институт связи

Непрерывная защита веб ресурсов

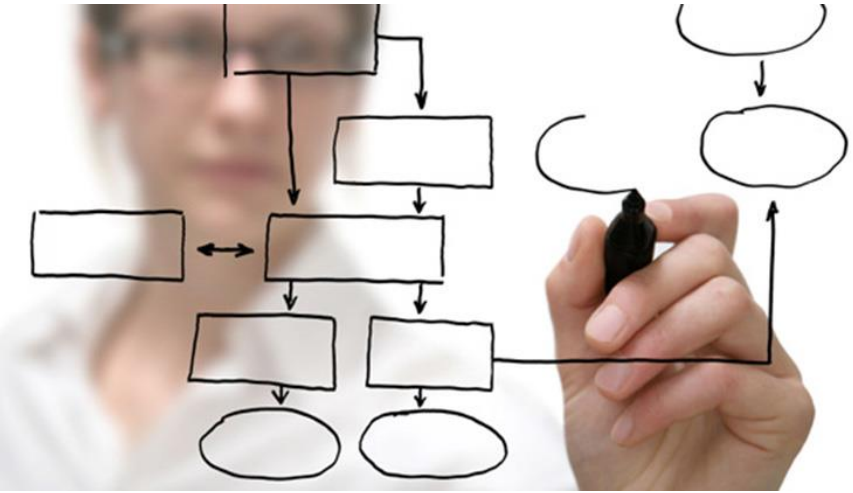


Злоумышленники имеют широкий набор инструментов для получения доступа к вашим веб-ресурсам и конфиденциальной информации постоянные обновления программного обеспечения добавляют ошибок — новых преимуществ вашим противникам в кибервойне. Реагировать на уже свершившиеся события неэффективно, неудобно и дорого. Необходимо комплексное решение, которое охватывает все этапы жизненного цикла веб-ресурса.

Центральный научно-исследовательский институт связи

Защита начинается на стадии разработки

Каждое веб-приложение содержит не **менее 5 критичных уязвимостей**, которые могут эксплуатировать хакеры. Используя ошибки в коде, хакеры получают контроль над ресурсом, доступ к базам данных, финансовым транзакциям, платежной, клиентской и другой конфиденциальной информации.

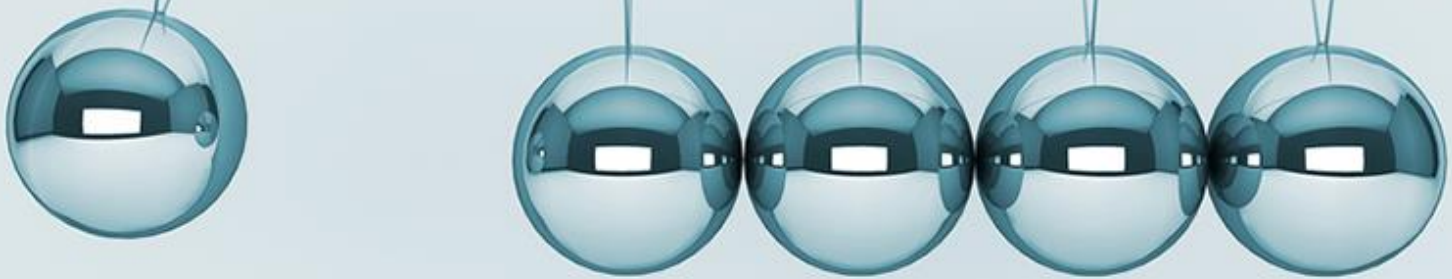


Каждое изменение ресурса несет потенциальную угрозу: новые строчки кода – со случайной ошибкой или специально оставленной закладкой, созданная учётная запись – со слабым паролем и чрезмерными пользовательскими привилегиями, новый бизнес-процесс – с новой схемой мошенничества. **Любые изменения объекта защиты влекут обязательную перенастройку систем безопасности.**

Центральный научно-исследовательский институт связи

Безопасность для непрерывности бизнеса

- **Непрерывная** активная и автоматическая **защита** для регулярно изменяющихся веб-ресурсов
- **Нивелирует человеческий фактор**



- Начинается на **стадии разработки**
- Обеспечивает **комплексную защиту** от сложных атак

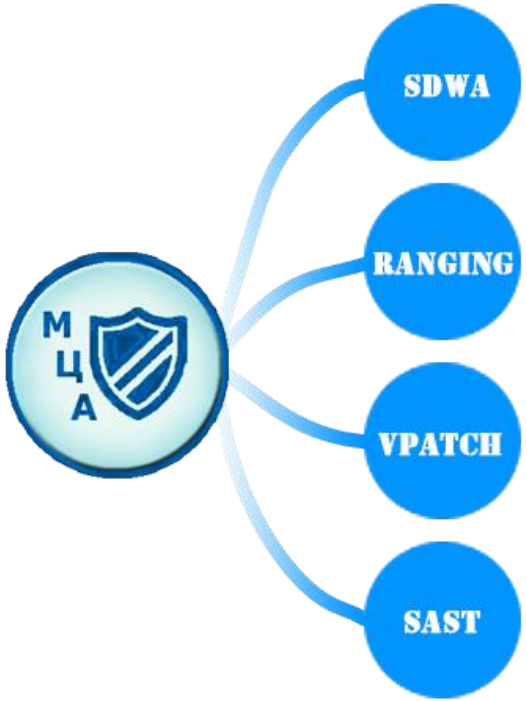
Центральный научно-исследовательский институт связи

Межоператорский центр анализа и мониторинга трафика (МЦА)

Основные функции и задачи МЦА

- ✓ Обеспечение необходимого уровня защиты инфраструктуры сети связи:
  - анализа поведения сети в реальном времени, создание критериев нормального поведения сети, приложений и действий пользователей
  - распознавания уже известных сигнатур, периодическое их обновление в случае обнаружения новых видов атак с повышенным риском применения
  - анализа безопасности используемых приложений и вычисление потенциальных угроз в приложениях
- ✓ Служба технической поддержки
  - круглосуточное экспертное обслуживание заказчиков по противодействию атакам для восстановления работы сети и услуг

Как это реализовано?



Интеллектуальная связка технологий
SAST + DAST + WAF + AntiDDoS

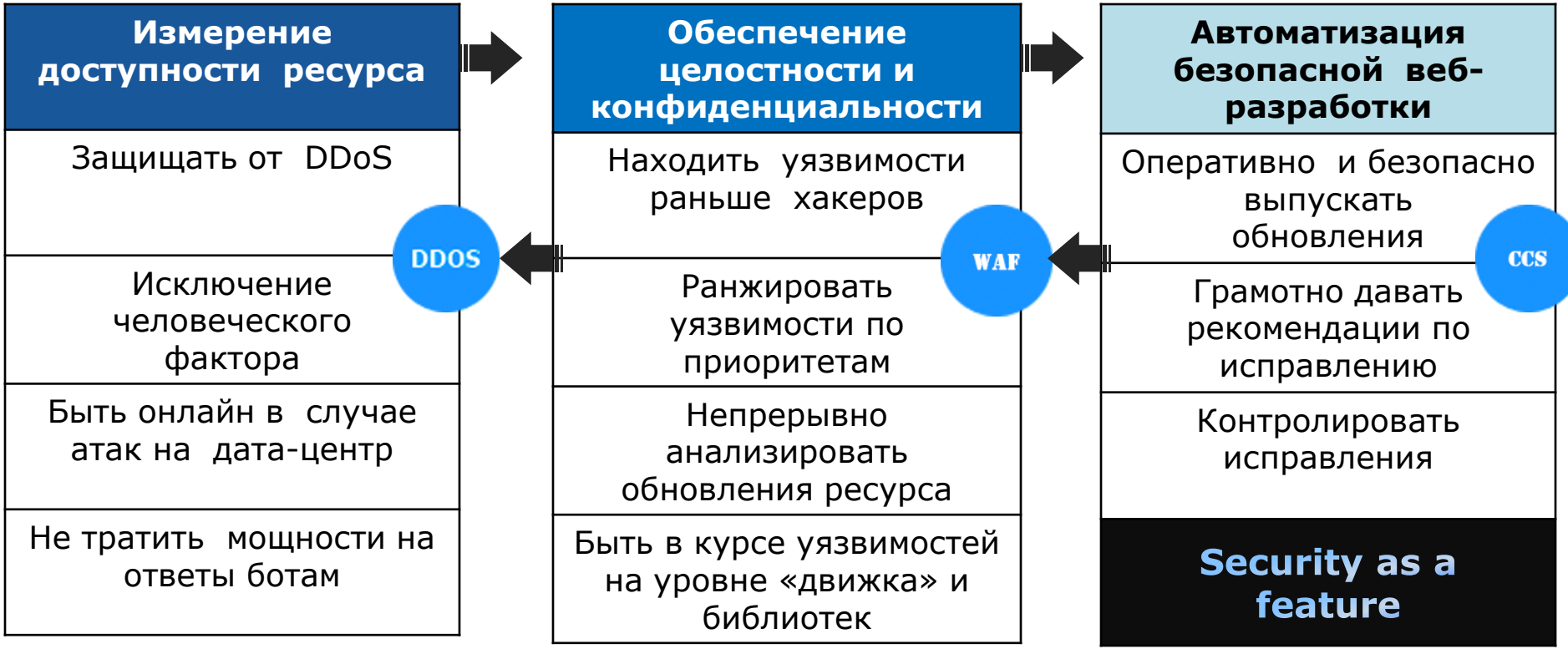
Наглядное ранжирование ошибок и рекомендации

Виртуальный патчинг до исправления

Проверка качества кода SAST

Карта задач и их решение

Центральный научно-исследовательский институт связи



Трафик в МЦА

Весь трафик, предназначенный для защиты, **постоянно** направляется через сеть фильтрующих узлов системы

Самообучение в нормальных условиях позволяет выявить аномалии и среагировать на новые виды DDoS

«Чистый» трафик передается клиенту либо через публичную сеть Интернет, либо через специальный выделенный канал

Центральный научно-исследовательский институт связи

Основные характеристики сети фильтрации

Около 1000 Гбит/с пассивной полосы пропускания

детерминированная обработка IP-пакетов без установления TCP соединения

Более 200 Гбит/с активной полосы пропускания каждое входящее TCP-соединение обрабатывается и анализируется

<1% ложных срабатываний

в процессе отражения DDoS-атаки

Время обучения с момента подключения менее 2 часов

в 33% случаев - до 4 минут

в 60% случаев - от 5 минут до 1 часа

Добавленное время задержки при проксировании трафика – от 0 до 100 мс

Центральный научно-исследовательский институт связи

Преимущества решения

Непрерывная защита от DDoS

С момента подключения ресурс компании находится под непрерывной защитой системы

Защита без дополнительных действий со стороны пользователя

Пользователи системы узнают о совершенных атаках только из утренних отчетов

Высокая пропускная способность

Канальная емкость сети и вычислительная мощность ее узлов способна обрабатывать 1000 Гбит трафика в секунду

Балансировка трафика клиента

Система обеспечит безотказную работу ресурса даже при проблемах с одним из серверов, используемых клиентом

Защита DNS-серверов, получение очищенного трафика через VPN MPLS L2, фильтрация HTTPS-трафика и др.

Центральный научно-исследовательский институт связи

Преимущества решения WAF

Непрерывная активная защита
Система находится в режиме активной защиты непрерывно

Локальный фильтрующий узел
Предотвращает хакерских атаки на веб-приложение и обнаруживает уязвимости веб-инфраструктуры

Машинное обучение
Позволяет автоматически адаптироваться к изменениям ресурса. Не требует ручной переконфигурации при каждом обновлении

Выявление многоступенчатых атак
На основе множества событий безопасности, фокусируя внимание на реальных угрозах (уязвимость + атака = инцидент)

Интеграция со статическим сканером
Совместное использование модуля Attack Killer Custom Code Scanner и встроенный динамический сканер приложений (SAST+DAST) минимизирует количество ложных срабатываний

Центральный научно-исследовательский институт связи

Преимущества решения Custom Code Scanner

Простой, быстрый инструмент,
не требующий настройки и затрат на поддержку

Обнаруживает ошибки в исходном коде
с учетом требований по безопасному программированию PCI DSS, OWASP, рекомендаций SDLC, а также производителей платформ

Поддержка языков
всех самых известных языков программирования (Java, PHP, JavaScript и др.)

Интеграция с WAF
позволяет избежать ложных срабатываний и построить процесс непрерывной безопасности: запросы на уязвимости, находящиеся на исправлении у разработчиков, автоматически блокируются модулем WAF

Центральный научно-исследовательский институт связи

Межоператорский центр анализа и мониторинга трафика (МЦА)

Результат

- ✓ Проактивная защита от DDoS атак
- ✓ Защита от атак на сеть ОКС7 оператора связи (подмена номера, определение местонахождения абонента через запрос IMSI, перехват SMS и вызовов абонента)
- ✓ Повышение стабильности функционирования информационно-телекоммуникационной инфраструктуры оператора связи
- ✓ Повышение доступности и качества оказываемых услуг

Спасибо за внимание!