Ростелеком
Солар

Технологии обеспечения кибербезопасности цифровой трансформации государства

Сергей Газизов
Заместитель директора по развитию региональных продаж
Компании «Ростелеком-Солар»

Текущая ситуация в киберпространстве

в 7 раз

выросло число кибератак

Самые атакуемые инфраструктуры:

22% Визитки госкомпаний и ФОИВ

16% ГИС с ПДн

15% Новостные издания и медиавещание

10% Сервисы для населения

7% Финансовые институты

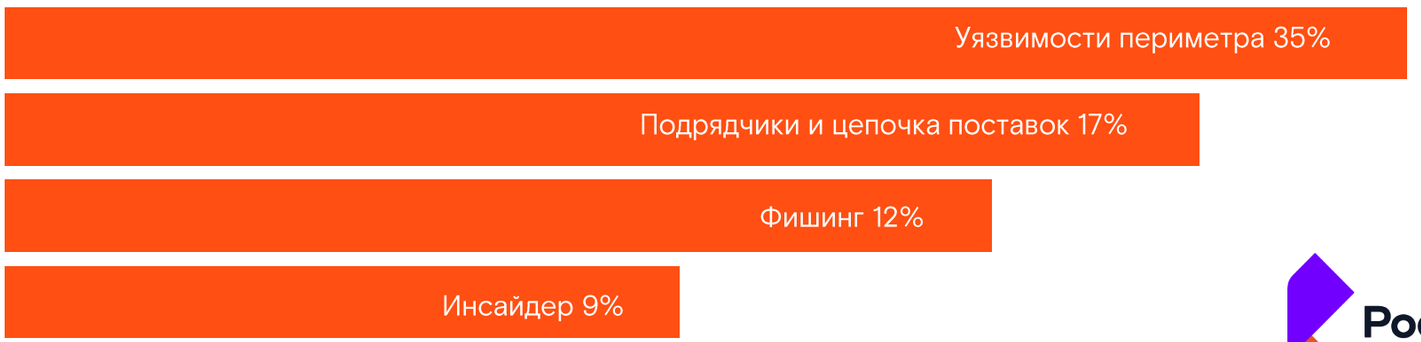
Число закладок в open-source:

30+ За март

100+ За июнь

- по данным «Ростелеком-Солар»

Основные векторы атак:



Ростелеком Солар

Уровни злоумышленников

УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
Киберхулиган/ энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
Киберкриминал/ организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО, доступные уязвимости, социнжиниринг
Кибернаемники/ продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
Кибервойска/ прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

Ростелеком Солар

Принципы обеспечения кибербезопасности

Для повышения защищенности при цифровизации организаций недостаточно линейного масштабирования традиционных подходов к кибербезопасности

Предпосылки

Размывание границ защищаемых сетей

Удаленные доступы и работа с домашних компьютеров, использование частных и публичных облаков

Усложнение и ускорение изменений в ИТ-ландшафте

До 10 новых релизов ИТ-систем в месяц, регулярный перенос новых функций ведомства в онлайн

Неэффективность стандартных СЗИ при современных атаках

Вредоносное ПО не детектируемое антивирусами, уникальные для каждой системы инструменты взлома

Использование сотрудников в качестве точки доступа в организацию

Сотрудники, администраторы и подрядчики – основные векторы взлома (через фишинг) и источники утечек информации

Недостаток квалификации и дефицит специалистов по кибербезопасности

Потребность в значительном расширении службы кибербезопасности, в том числе в регионах, организации выполнения большинства функций 24/7

Повышение эффективности

1. Безопасность через мониторинг и управление
2. Безопасность через контроль действий пользователей и админов
3. Безопасность через системное обучение и воспитание персонала

Ростелеком Солар

Комплексная кибербезопасность

Ростелеком Солар

Решение задач государственных организаций

За счет собственных разработок

- Защита от утечек информации
- Контроль соблюдения Кодекса этики и служебного поведения служащих
- Реализация политики использования сети «интернет»
- Управление доступом к информационным системам
- Контроль безопасности кода

За счет собственных сервисов

- Раннее предупреждение, выявление и реагирование на кибератаки
- Оценка рисков и управление уязвимостями
- Шифрование каналов связи
- Повышение квалификации и осведомленности сотрудников
- Защита веб-порталов и приложений

За счет интеграционных услуг

- Комплексный подход к решению задач кибербезопасности
- Защита ГИС и их аттестация в соответствии с требованиями регуляторов
- Защита периметра, ИТ-инфраструктуры, рабочих станций, ЦОД
- Обеспечение выполнения требований законодательства

Ростелеком Солар

Импортозамещение: есть работающие практики

01 Анализ существующей инфраструктуры, выявление иностранных средств защиты, требующих оперативной замены

02 Подбор альтернативных отечественных продуктов с необходимым функционалом

03 Функциональное тестирование подобранных решений в демолаборатории

04 Внедрение российских аналогов в текущую инфраструктуру

05 Перенос политик и правил на новые средства защиты

06 Проверка доступности сервисов компании

07 Перевод в промышленную эксплуатацию

08 Оценка соответствия настроек средств защиты лучшим практикам и собственным политикам безопасности

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru