Памятка[1] по обеспечению безопасности и доступности информационных систем в условиях непрерывных кибератак

Убедительная просьба к руководителям организаций, руководителям служб безопасности, а также всем, кто осуществляет взаимодействие с внутренними информационными системами, отслеживать вредоносную активность, а также иные виды информационных атак. При отсутствии внутренних процессов для решения этих задач, как можно скорее обращайтесь к специалистам и компаниям по кибербезопасности.

Текущие атаки на информационные ресурсы Российской Федерации

Фишинговые атаки

1. Сотрудникам, обрабатывающим электронные письма, быть внимательными к вложениям и внешним ссылкам в теле письма и ни в коем случае не переходить по ним, если отправитель вам неизвестен и если отсутствует крайняя необходимость.
2. Проверять адрес отправителя. Должны вызывать подозрения домены по типу `support@go0gle.com, noreply@vk.restore-password.ru.`
3. Обновить антивирусное программное обеспечение до актуального состояния.

Атаки отказа в обслуживании (DoS/DDoS)

1. Усилить мониторинг узлов сети смотрящих наружу в сеть Интернет.

Атаки на веб-приложения

1. Провести тесты на проникновение всех веб-приложений и сервисов компании, доступных из сети Интернет. Также провести автоматизированное сканирование уязвимостей.
2. Временно ограничить доступ к ресурсам только с IP-аресов Российской Федерации, если не критично взаимодействие с зарубежными пользователями.

Правила поведения на рабочих местах

1. Ограничить посещение сторонних ресурсов, ограничившись только работой с информационными системами, расположенными в Российской Федерации.
2. Исключить использование социальных сетей и мессенджеров на рабочих местах, если это возможно.
3. Убедиться в том, что в открытом доступе не хранится чувствительная информация о сотрудниках и/или инфраструктуре (это можно сделать, заказав у ИБ-компании услугу по снятию цифрового отпечатка).

1 Памятка подготовлена в рамках аналитической работы, проделанной на основе фактологической информации, приведенной в **Приложении 1**.

Рекомендации по укреплению защиты информационного периметра

В связи с вышесказанным мы настоятельно рекомендуем проводить ряд мероприятий по обеспечению безопасности информационного периметра организации, а именно:

1. Обеспечить периодическое сканирование уязвимостей информационного периметра организации. При таком сканировании, в том числе, необходимо использовать специализированные сканеры для веб-ресурсов и «чекеры» для проверки наличия свежих уязвимостей с высоким уровнем опасности.
2. Обеспечивать использование стойких паролей для учётных записей сотрудников, получающих доступ к информационным ресурсам. Проверка паролей должна осуществляться на техническом уровне по словарям, паттернам парольных политик и т. д.
3. Обеспечить использование механизмов двухфакторной аутентификации на всех информационных ресурсах внешнего периметра, для которых это возможно.
4. Обеспечить безопасную публикацию информационных ресурсов с использованием технологий WAF, Reverse proxy и выделенного сегмента сети (DMZ).
5. Внедрить периметральные средства интеллектуального межсетевого экранирования и защиты от сетевых угроз (DPI, NGFW, NTA, IPS).
6. Внедрить технологии проверки безопасности канала получения электронной почты. Для этого рекомендуется использовать антивирус, анти-спам и технологий песочницы, а также обязательно провести киберучения и имитацию рассылок заражённых писем.

Случаи обнаружения успешного проникновения в инфраструктуру

Если был обнаружен и подтверждён «пробив» периметра сети организации и/или обнаружено, что *в данный момент* злоумышленники «работают» в ней, необходимо срочно предпринять ряд мероприятий, направленных на минимизацию рисков и выдворение «непрошенных гостей» за пределы сетевой инфраструктуры.

1. Используя средства мониторинга и журналирования, необходимо реконструировать вектор проникновения злоумышленников, выявить и изолировать сетевой сегмент и/или систему, подверженную компрометации.
2. Необходимо устранить выявленную брешь периметра, через которую злоумышленникам удалось проникнуть в сеть организации. Это может быть уязвимый внешний сервис (например, веб-сервис, подверженный уязвимости `Log4j`, или Microsoft Exchange, подверженный уязвимости `ProxyLogon`), фишинговое письмо, VPN, любая технология удалённого доступа и т. д.
3. По возможности следует провести сетевую локализацию скомпрометированного сегмента сети.

Контроль применения иностранных программного и/или аппаратного обеспечения

Необходимо разработать план работы в случае выхода из строя или прекращения работы оборудования и программного обеспечения иностранного производства. Следует произвести отказоустойчивость за счёт дублирования функций на базе отечественных аналогов.

Контроль использования каналов связи иностранными программным и/или аппаратным обеспечением

Рекомендуется использовать технологии глубокой инспекции трафика (DPI) для определения потенциального использования недокументированных возможностей (НДВ), осуществлять анализ использования памяти, обращение к процессам и дисковому пространству для программного обеспечения и оборудования иностранного производства.

Приложение 1 – Официальные сообщения об угрозах ИБ

Созданный по приказу руководства ФСБ Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупредил об угрозе увеличения интенсивности компьютерных атак на российские информационные ресурсы, в том числе объекты критической информационной инфраструктуры (КИИ) на фоне проводимой военной операции на Украине.

> «*Атаки могут быть направлены на нарушение функционирования важных информационных ресурсов и сервисов, нанесение репутационного ущерба, в том числе в политических целях. Кроме того, в дальнейшем возможно проведение вредоносных воздействий из российского информационного пространства для формирования негативного образа Российской Федерации в глазах мирового сообщества*» – НКЦКИ.

Специалисты НКЦКИ рекомендуют российским организациям усилить бдительность при мониторинге вредоносной активности, направленной на объекты, находящиеся в зоне ответственности организации, организовать процесс приоритетной обработки информации об аномалиях, обнаруживаемых в работе объектов КИИ.

НКЦКИ также был выпущен бюллетень о растущей киберугрозе.

2 высокопоставленных человека из разведки США предложили два плана по кибератакам на Российскую Федерацию.