IS RISKS – отправки инфраструктурных данных для мониторинга инфраструктуры ОКИИ

ИБ предлагает принять целевые риски активности с учетом реализации мер ИБ		Текущий уровень в активности	Целевой уровень в активности	Контрольная среда
NC	**Нарушение законодательных требований** 187-ФЗ к защите данных ОКИИ, что может привести к административной ответственности со стороны ФСТЭК, вплоть до уголовной (при причинении значимого вреда КИИ).	H	M	
DL	**Утечка конфиденциальной информации** в логах совершенная из внешней неконтролируемой среды , что может привести к ущербу репутации, компрометации инфраструктуры и, как следствие, усилению кибер-атак на ОКИИ	H	M	

Не отображены риски, на которые активность не имеет значимого влияния

Основные меры защитs

PRE-условия	Ответственный	Статус	Срок
Провести сканирование исходного кода системы мониторинга			
Обезличить инфраструктурные данные, которые передаются в виде нотификаций в телеграмм канал			
Проработать и автоматизировать механизм удаления чувствительных данных из системы мониторинга, telegram-канала раз в неделю			
Интегрировать систему мониторинга с telegram-каналом для передачи инфраструктурных логов через WSO2 MI			

POST-условия	Ответственный	Статус	Срок
Устранить уязвимости по отчету сканирования исходного кода системы мониторинга			
Проработать возможность использования отечественного аналога telegram на других платформах и согласовать с ИБ			
Реализовать механизм защиты микросервисов и контейнеризации на OpenShift			
Проработать ролевую матрицу системы мониторинга и согласовать с BISO			
Интегрировать DAM и обеспечить контроль трафика на PROD сервере			
Провести Hardening платформы PostgreSQL в соответствии с CIS Benchmarks			

Vulnerability Description NC (HIGH): Нарушение требований к защите КИИ (к применяемым программным средствам, к информационному взаимодействию с иными информационными системами, информационно-телекоммуникационными сетями и т.д.) в следствии нотификаций инфраструктурных логов в telegram чат - незащищенный канал передачи данных, который не контролируется средствами и методами СЗИ.

Threat Description: Идентификационные данные hostname, environment, ip-адреса, ТУЗ, etc., при раскрытии, позволяют эксплуатировать злоумышленником 0-day уязвимостей, реализовать DoS, etc., что вследствии приводит к причинению вреда ОКИИ при нарушения требований к защите КИИ.

Scenario Impact Description: В случае раскрытия конфиденциальной информации уровня С2 (инфраструктурные логи) повлекшей за собой киберинцидент на ОКИИ, либо проведении регуляторной проверки, аудита (включая/исключая киберинцидент) возможно выявление несоответствия требований к защите ОКИИ, что приведет к штрафным санкциям для ОКИИ, должностных лиц, в том числе уголовную ответственность.

Санкционный риск связанный с штрафами от регуляторов по факту совершенного киберинцидента, где передается информация в НКЦКИ для проведения расследования и вынесения соответствующей ответственности для ОКИИ, должностных лиц. Риск может повлечь за собой проверку на соответствие другим требованиям к защите ОКИИ. В случае выявления аудитом, либо регуляторной проверки ответственность аналогична, отличия в степени тяжести по действующему законодательству.

Санкционный риск включает в себя нарушение условий кризисных требований:

- Письмо ФСТЭК, - запретить возможность размещения защищаемой информации в облачных сервисах, а также ее передачу через мессенджеры, Google Docs и другие сервисы,
- Письмо ФСТЭК, - провести инвентаризацию информационных ресурсов на предмет использования иностранного программного обеспечения, включая облачные решения, мессенджеры, системы управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисное программное обеспечение, интегрированную среду разработки (IDE). В случае наличия таких решений разработать план по переходу на отечественные аналоги,
- Бюллетень НКЦКИ, - организовать инвентаризацию облачных решений и разработать план по переходу на Российские аналоги или решения, разворачиваемые локально и неконтролируемые производителем извне. Это касается в том числе и решений, которые используются коммерческими предприятиями: мессенджеры, система управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисные пакеты, интегрированные среды разработки (IDE) и прочее.

Аналогично: РКН признал Telegram иностранным мессенджерам и не подлежащим к интеграции с ОКИИ.

Ответственность:
УК согласно ст. 274.1 УК РФ, части 3,4,5
Сроком лишения свободы до 10 лет,
Запрет на деятельность и занимаемые должности до 5 лет для должных лиц.
ГК - КоАП РФ Статья 13.12.1. с штрафом до 100 000 рублей на физическое лицо, на юридическое лицо до 500 000 рублей,
Иные регуляторные штрафные санкции для ОКИИ.

Последовательность: уведомление о устранении (в случае отсутствия киберинцидента), штрафы, привлечение к ответственности согласно УК, ГК РФ.

Vulnerability Description DL (HIGH): Утечка конфиденциальной информации в логах через telegram-канал совершенная сотрудниками банка без умысла по неосторожности, не должной осмотрительности, а также использования на личных локальных машинах, повлекшая к компрометации инфраструктуры.

Threat Description: Идентификационные данные hostname, environment, ip-адреса, ТУЗ, etc., при раскрытии, позволяют эксплуатировать злоумышленником 0-day уязвимостей, реализовать DoS, украсть конфиденциальную информацию ОКИИ, клиентов, etc.

Scenario Impact Description: Реализация путем социальной инженерии, отсутствие САВЗ на личных устройствах, утери оборудования, потери права владения УЗ в месенджере/почте/номера телефона (отсутствие PIN на сим-карте), etc., что приводит к компрометации инфраструктурных данных и к возможности реализации расширенного вектора атак на ОКИИ: применение шифровальщиков, реализации 0-day уязвимостей ПО, подмены конфигурации, исследованию работ приложений банка, etc., что вследствии может привести к утечке данных, DoS, негативным репутационным последствиям.

Vulnerability Description CR (Medium): Киберпреступления, совершенные третьими лицами, в отношении telegram-чата приведшая к утечке конфиденциальной информации..

Threat Description: Идентификационные данные hostname, environment, ip-адреса, ТУЗ, etc., при раскрытии, позволяют эксплуатировать злоумышленником 0-day уязвимостей, реализовать DoS, украсть конфиденциальную информацию ОКИИ, клиентов, etc.

Scenario Impact Description: При компрометации внешнего партнера возможна утечка конфиденциальной информации третьим лицам, а также публичность инфраструктурных данных ОКИИ в сообществах, что привлечет интерес внешних злоумышленников и сканированию инфраструктуры, включая воздействия на фрод-чувствительные ИС.

Vulnerability Description UN (Medium/LOW): Саботаж внутренних ИТ-систем путем эксплуатация конфиденциальной инфраструктурной информации (hostname, ip, etc.) ОКИИ, который привел к прерыванию работы операционных процессов или ухудшению качества оказания услуг клиентам, которая была намеренно совершена для получения личной выгоды, либо инсайдерской информации.

Threat Description: Идентификационные данные hostname, environment, ip-адреса, ТУЗ, etc., при раскрытии, позволяют эксплуатировать злоумышленником 0-day уязвимостей, реализовать DoS, украсть конфиденциальную информацию ОКИИ, клиентов, etc.

Scenario Impact Description: Саботаж для достижения личной выгоды путем замедления бизнес процессов, либо получения информации необходимой для инсайдерской продажи, либо эксплуатации DoS, либо повышения показателя эффективности, etc, которые могут привести к перебоям в обслуживании, утери данных, либо подмене данных, модификации путем определения конкретных конфигураций ИС.