ИССЛЕДОВАНИЕ

АТАКИ ИНСАЙДЕРОВ: УГРОЗА ВНУТРИ ПЕРИМЕТРА

SECURITY TEAM

JET SECURITY TEAM

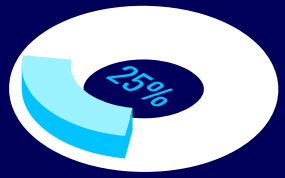
Оглавление

Ключевые цифры

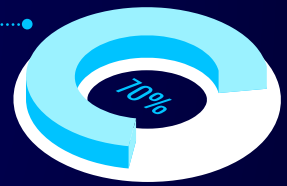
С начала 2023 года Jet CSIRT наблюдает системный рост инсайдерских атак от рядовых пользователей: количество таких инцидентов увеличилось в **1,5 раза** по сравнению с аналогичным периодом прошлого года

Почти половина опрошенных **(43%)** не применяют мер усиленного контроля в отношении сотрудников из групп риска (работники, которые скоро уволятся, и работники подрядчика, договор с которым вскоре закончится)

Анализ уникальных сообщений о сделках в Даркнете показал, что за первое полугодие 2023 года спрос на инсайдерскую информацию вырос почти на **25%**



По опыту проведения экспертных аудитов, у порядка **70%** компаний обнаруживаются критичные недостатки в процессе управления доступом.



На **83%** проектов по внутреннему пентесту нам удается получить доступ к особо чувствительным данным компании, не прибегая к повышению привилегий — под учетными записями рядовых работников, для которых такой доступ является избыточным

Аннотация

Исследование посвящено анализу инсайдерских угроз — использованию персоналом легитимного доступа с целью нанесения вреда компании, ее системам, оборудованию, информации или репутации.

Цели исследования:

- Обозначить основные угрозы, источниками которых являются инсайдеры
- Выявить ключевые недостатки в защите от инсайдеров
- в российских компаниях
- Оценить готовность российских компаний к противодействию таким угрозам
- Дать рекомендации по защите от инсайдерских угроз

Основу исследования составили:

- Данные и кейсы, полученные в ходе реализации проектов по аудиту информационной безопасности, тестированию на проникновение
- Результаты мониторинга и реагирования на инциденты в рамках оказания сервисов SOC со стороны команды мониторинга Jet CSIRT
- Результаты расследования компьютерных инцидентов со стороны экспертов по форензике
- Аналитика, полученная по результатам работы группы мониторинга внешних цифровых рисков
- Информация, полученная в ходе реализации проектов по внедрению и настройке средств защиты, в частности, на проектах внедрения DLP, DCAP/DAG, UEBA/UBA, систем по маркировке электронных документов

Концепция и методология

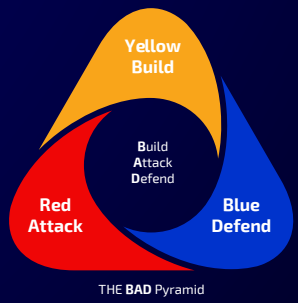
Для того чтобы лучше понять, как реализуются инсайдерские угрозы, Агентством национальной безопасности (NSA) была разработана цепочка «Insider Kill Chain», основанная на модели The Cyber Kill Chain и проекте MITRE ATT&CK (подробнее в разделе «Как действуют инсайдеры»). Цепочка содержит четыре этапа, по которым инсайдеры могут действовать внутри инфраструктуры для достижения своей цели.

В рамках отчета последовательно рассмотрены каждый из этапов данной цепочки в контексте:

1. Чем характеризуется этап: краткое описание
2. Что мы наблюдаем: аналитика по результатам реализации проектов и оказания сервисов в области кибербезопасности
3. Кейсы: примеры инцидентов, демонстрирующих типовое поведение инсайдера на данном шаге
4. Результаты опроса: выводы по результатам опросов ключевых заказчиков АО «Инфосистемы Джет» и внешней профильной аудитории
5. Как защититься на этом этапе: меры и средства защиты, минимизирующие риски или полностью предотвращающие дальнейшее проведение атаки

Аналитика в рамках каждого этапа предоставлена участниками трех основных команд (согласно принципу BAD Pyramid):

- проектирующих и строящих системы защиты (Yellow Team)
- атакующих (Red Team)
- защитников (Blue Team)



THE **BAD** Pyramid

Введение

Одна из распространенных причин утечек данных — работники компании, которые используют данные в рамках выполнения должностных обязанностей. Согласно отчету Verizon 2023 Data Breach Investigations Report [1], **19%** утечек конфиденциальной информации связаны именно с внутренними нарушителями.

При этом в **74%** случаев причиной являлся человеческий фактор (включая атаки социальной инженерии, неправильное использование, злоупотребление привилегиями и использование украденных учетных данных).

Инсайдерские атаки — несанкционированные действия работников компании, при выполнении которых работник имеет легальный доступ к системам и инфраструктуре и/или в помещения компании. При таких условиях работник может осознанно злоупотреблять своими правами доступа или неосознанно совершать ошибки, наносящие ущерб компании[2].

Являясь далеко не самыми массовыми, инсайдерские угрозы в случае реализации наносят наиболее ощутимый и дорогостоящий ущерб организации, который может включать в себя:

- утрату конфиденциальной информации и интеллектуальной собственности;
- финансовые потери из-за кражи денег или мошенничества;
- убытки из-за прерывания бизнес-процессов или выхода из строя систем;
- репутационный ущерб из-за утечки данных или других инцидентов.

К инсайдерам можно отнести следующих лиц:

- текущие работники компании, в том числе имеющие привилегированные права доступа;
- бывшие работники компании;
- работники подрядчика, имеющие доступ к корпоративным ресурсам;
- работники дочерних организаций, имеющие доступ к совместным ресурсам.

[1] https://www.verizon.com/business/resources/Tc42/reports/2023-data-breach-investigations-report-dbir.pdf

[2] В рамках проводимого исследования не учитывались угрозы, связанные с финансовым мошенничеством, т. к. данная тема заслуживает отдельного исследования

Типы инсайдеров:

Нарушитель «по незнанию»

Отсутствует мотивация нанести вред компании, из-за невнимательности/незнания корпоративных политик кибербезопасности его действия могут привести к инциденту: сторонние получатели в письме, отправка на личную почту, в мессенджеры, на личные съемные носители или в облачные хранилища конфиденциальных материалов, чтобы поработать из дома / «на всякий случай».

Такие кейсы мы систематически наблюдаем в рамках проектов по сопровождению DLP-систем. Например, работница компании отправила на внешний адрес отчеты с закрытой финансовой информацией. При детальном расследовании инцидента оказалось, что у сотрудницы не было злого умысла, и причиной инцидента была невнимательность (работница не проверила адрес получателя, считая, что отправляет информацию своим коллегам).

Нелояльные инсайдеры

Реализовывают свои действия намеренно и с полным пониманием последствий. Основной мотив — не личная выгода, а желание навредить компании. Причинами могут стать неудовлетворенность уровнем заработной платы или текущей должностью, конфликты в коллективе и др. В случае наличия у такого работника суперполномочий в системах компании его действия могут привести к нарушению операционных процессов.

Так, в одной из компаний системный администратор при увольнении изменил пароли на всём оборудовании и на всех серверах, где у него были права. Восстановление доступа заняло огромное количество времени, что привело к простою ряда бизнес-процессов, невозможности штатного резервирования данных и технической поддержки пользователей.

Инсайдеры, нацеленные на собственную выгоду

Скачивают конфиденциальную информацию компании с целью получения личной выгоды: для развития собственного бизнеса, получения материальных выплат от третьих лиц, заинтересованных в конкурентном преимуществе, а также хищения денежных средств.

На одном из внедрений в рамках мониторинга поступающих событий был выявлен следующий критичный инцидент: работник отправил на корпоративный съемный носитель порядка 2 000 документов, которые содержали чертежи, технические условия, информацию о коммерческой деятельности компании, информацию о выручке компании и часть текстов договоров с контрагентами. Он планировал скопировать полученную информацию на домашний компьютер, а съемный носитель сдать во время подписания обходного листа, удалив скопированные данные. Как выяснилось позднее, сотрудник планировал открыть собственный бизнес в смежной сфере.

Насколько это актуально?

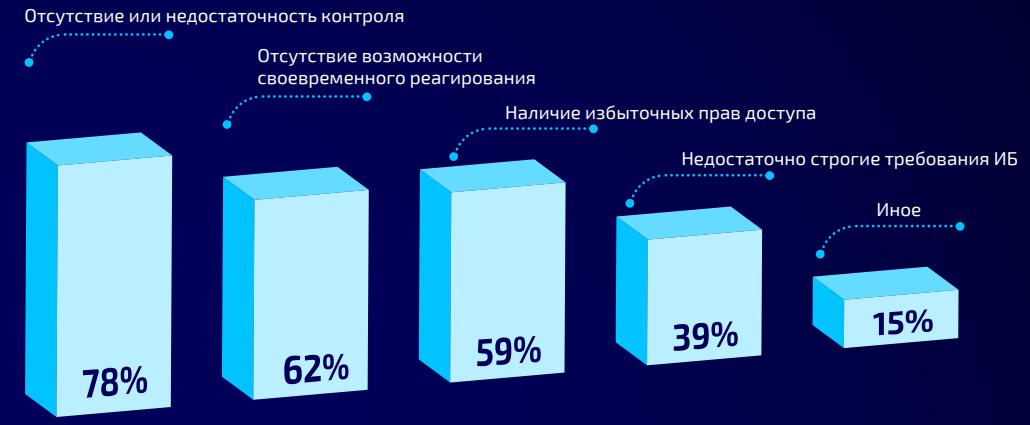
При мониторинге форумов Даркнета и некоторых Telegram-каналов наблюдался постоянный спрос на покупку и предложения на продажу инсайдерской информации. Объявления данной направленности составляют около трети всех предложений на теневом рынке, к ним относятся: покупка/продажа корпоративных доступов к виртуальным серверам, баз данных различных компаний, а также поиск действующих сотрудников компаний, готовых сотрудничать со злоумышленниками. Уникальными и редкими являются предложения о продаже доступа к административным учетным записям.

Для более комплексного анализа инсайдерских угроз и их актуальности мы попросили наших респондентов ответить на несколько вопросов. В опросе приняли участие более 80 компаний, среди которых представители крупного бизнеса (большинство), а также малые и средние предприятия и организации госсектора.

Почти половина **(47%)** опрошенных компаний сталкивались за последний год как минимум с одним инцидентом информационной безопасности, связанным с действиями инсайдеров.

Были ли в компании за последний год инциденты, связанные с действиями инсайдеров?

ТОП-3 наиболее опасных инсайдеров для компаний составляют текущие работники, работники компании, имеющие привилегированные права доступа, и работники подрядчика, имеющие доступ к корпоративным ресурсам. Основными причинами успешной реализации несанкционированных действий инсайдеров, по мнению респондентов, являются отсутствие или недостаточность контроля, отсутствие возможности своевременного реагирования и наличие избыточных прав доступа.



Что, на ваш взгляд, является ключевыми причинами успешной реализации несанкционированных действий инсайдеров?

Какой тип инсайдеров наиболее опасен для вашей компании?

Историческая справка

Публичные инциденты, произошедшие в 2022 году и первой половине 2023 года, иллюстрируют актуальность угроз, связанных с инсайдерами. Вот лишь некоторые громкие инциденты:

01.03.2022

Яндекс.Еда сообщила об утечке данных пользователей сервиса, которая включала в себя персональные данные пользователей. Как сообщила сама компания, инцидент произошел в результате недобросовестных действий одного из сотрудников, из-за которых данные пользователей попали в общий доступ.

19.12.2022

В декабре 2022 года стало известно о признании бывшего работника Twitter виновным в осуществлении шпионажа за пользователями социальной сети. Работая в компании, он передавал Саудовской Аравии личные данные пользователей.

26.01.2023

Была опубликована ссылка на скачивание дампа, полученного из внутреннего репозитория компании «Яндекс». Дамп содержал исходные коды нескольких продуктов и сервисов компании. В СМИ утверждается, что файл был передан анонимному пользователю хакерского сайта BreachForums от «недовольного сотрудника» компании.

21.08.2023

Tesla сообщила об утечке данных, которая затронула более 75 000 текущих и бывших сотрудников. По данным внутреннего расследования, причиной утечки стали двое бывших работников компании, которые направили 100 Гб информации из внутренних систем компании в СМИ. В составе разглашенной информации были имена, адреса, телефоны и номера социального страхования.

19.09.2023

Сотрудник компании Microsoft непреднамеренно выложил в общий доступ 38 ТБ информации, включающей в себя приватные ключи, пароли, резервные копии персональных компьютеров работников Microsoft и более 30 000 внутренних сообщений из корпоративного мессенджера. Помимо чтения указанной информации, у злоумышленников была потенциальная возможность удалять и перезаписывать существующие файлы. Произошло это из-за некорректной конфигурации токена SAS (Shared Access Signature).

Как действуют инсайдеры — Insider Kill Chain

Последовательность шагов инсайдерской атаки может значительно отличаться от классических моделей, таких как MITRE ATT&CK и Lockhead Martin Kill Chain. Дело в том, что инсайдерские угрозы не всегда связаны с хакерскими действиями или техническими методами взлома, а включают также социальные, психологические и организационные аспекты. Находящемуся во внутренней инфраструктуре инсайдеру необходимо выполнить меньше шагов, чтобы добиться своей цели.

Инсайдерская цепочка (Insider Kill Chain) — концепция, описывающая последовательность этапов, которые могут быть использованы инсайдерами (внутренними сотрудниками или другими уполномоченными лицами) для совершения кибератак или утечки информации. Эта модель анализирует шаги, которые инсайдеры могут предпринять, начиная от планирования и заканчивая действиями, направленными на достижение цели. Insider Kill Chain уделяет особое внимание действиям инсайдеров внутри организации, тогда как другие модели описывают широкий спектр тактик и техник, используемых злоумышленниками, независимо от того, являются ли они внутренними или внешними злоумышленниками.

При создании сценариев выявления инцидентов в центре мониторинга и реагирования Jet CSIRT мы используем два подхода: классический маппинг угроз на MITRE ATT&CK и дополнительный маппинг угроз на «инсайдерскую цепочку» (Insider Kill Chain). Меры предотвращения, обнаружения и реагирования для инсайдерской цепочки атаки включают в себя использование как технических, так и организационных и правовых методов защиты.

Рекрутинг / Переломный момент

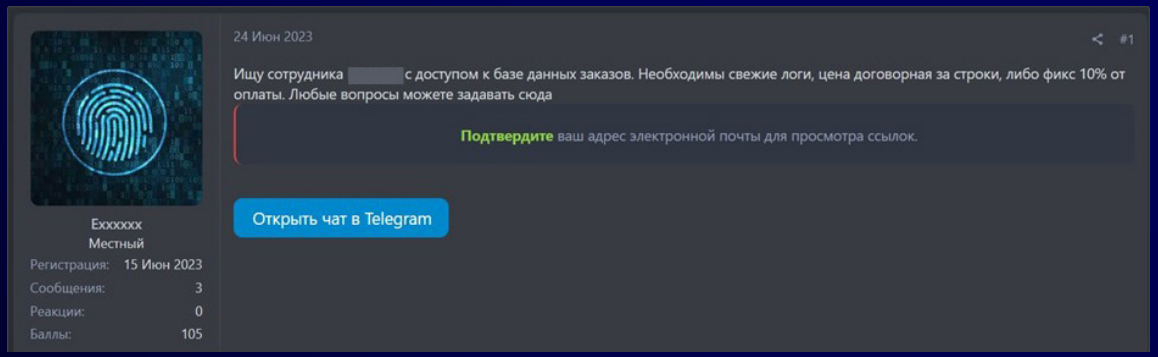
На этом этапе случается «переломный момент», после которого инсайдер начинает рассматривать возможность совершения незаконных или вредоносных действий внутри организации (например, ищет способы продажи данных в Даркнет). Отследить этот этап средствами мониторинга крайне тяжело или даже невозможно. Данный этап применим именно для мотивированных инсайдеров.

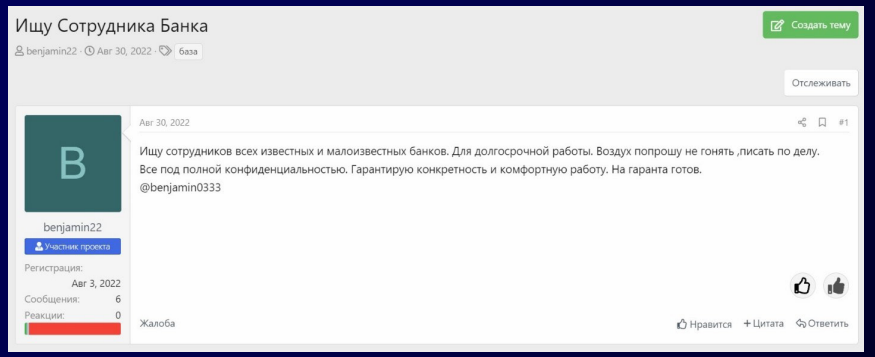
Что мы наблюдаем

Существует несколько вариантов развития событий, когда инсайдер приходит в Даркнет: он либо размещает объявления о своих услугах, либо ищет действующие предложения о сотрудничестве. Такие предложения, как правило, включают продажу критичных данных или заказ на «взлом» с уничтожением данных или заражением инфраструктуры вредоносным ПО. На форумах ежедневно появляются сотни предложений о «вербовке» сотрудников, в таких предложениях злоумышленники готовы работать с ними на постоянной основе. Если сделка о сотрудничестве совершилась, то компания не сразу заметит пропажу данных, так как информация будет сливаться хоть и регулярно, но не в огромном объеме, как это бывает с утечками баз данных в общий доступ. Ниже представлены некоторые примеры подобных предложений.

Анализ уникальных сообщений о сделках в Даркнете показал, что за первое полугодие 2023 года спрос на инсайдерскую информацию вырос почти на 25%. В целом на протяжении последних нескольких лет картина с покупкой и продажей такого вида информации значительно не меняется, спрос и предложения есть всегда. Растут цены, но это скорее связано с общей инфляцией и политической ситуацией в стране. Цены зависят от разных факторов, таких как актуальность и уникальность информации, объем данных и т. д., и могут варьироваться от нескольких тысяч рублей до сотен тысяч долларов.

Как показывает наша практика, сервисы/услуги по мониторингу поверхности атаки (сервисы киберразведки) используются всего в **11%** компаний.

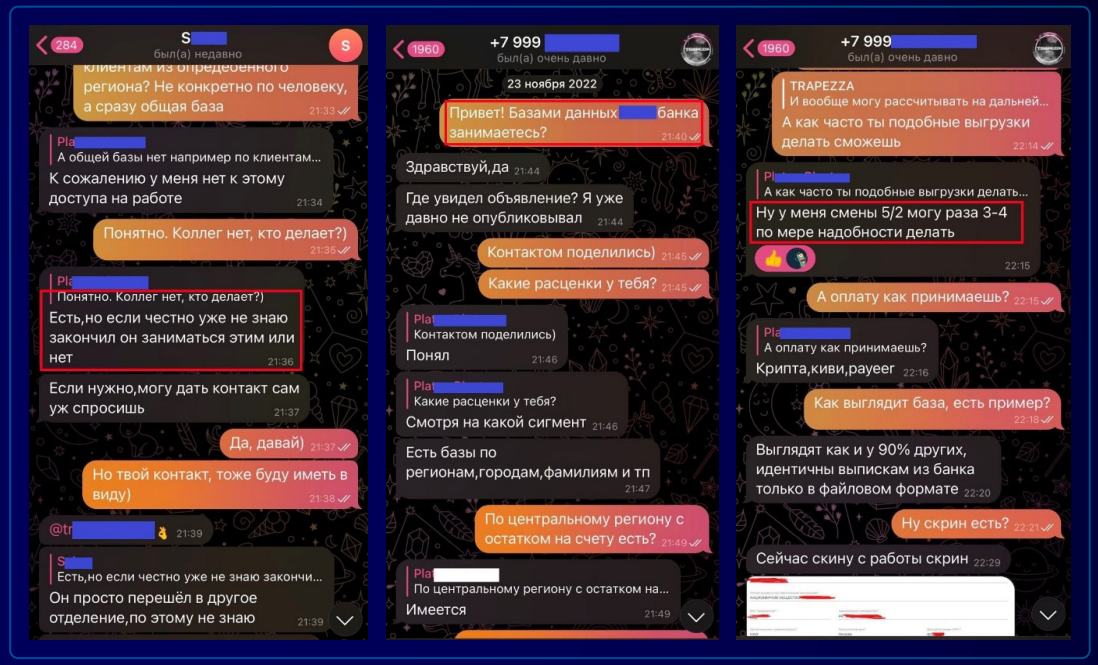




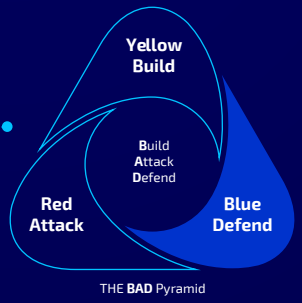
JET SECURITY TEAM

Кейсы

В ходе легендированной переписки был найден сотрудник одного из популярных банков, который на постоянной основе был готов выгружать базы клиентов банка по запросу с необходимыми для злоумышленника данными. В примере базы была информация о владельце счета, его родственниках, даты и места оформления договоров и карт, остаток на балансе, включая выписки за три месяца, последние транзакции, информация о тратах за последний месяц, информация о блокировках и ограничениях, информация по кредитной истории и кредитных картах.



В данном кейсе продемонстрирован один из многих возможных примеров успешного рекрутинга, который показывает, насколько быстро и просто злоумышленник может договориться с нелояльным сотрудником.

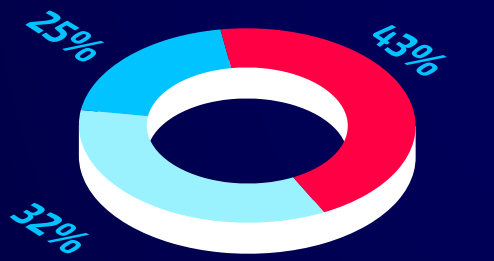


THE **BAD** Pyramid

Результаты опроса

Несмотря на то, что в основную зону риска входят, как правило, увольняющиеся работники/внешние подрядчики, практика их мониторинга не распространена в российских компаниях: почти половина опрошенных **(43%)** не применяет усиленных мер контроля в отношении данных групп риска. Режим блокировки выхода конфиденциальной информации за периметр на системах DLP используют только четверть опрошенных – **25%**

Предусмотрены ли в компании меры усиленного мониторинга (мониторинга всех действий) для работников, которые скоро уволятся/работников подрядчика, договор с которым скоро закончится?



- Да, до увольнения контролируются все каналы передачи информации для таких пользователей с блокировкой потенциально опасной передачи
- Да, до увольнения контролируются все каналы передачи информации для таких пользователей в режиме мониторинга
- Меры усиленного мониторинга не применяются

Каким образом осуществляется предупреждение работников компании / работников подрядчиков об ответственности за разглашение конфиденциальной информации?

С целью предупреждения об ответственности основной практикой является подписание NDA с работниками и юридическим лицом — ее используют большинство опрошенных. При этом только **4%** компаний не предпринимают никаких мер.

Как защититься на этом этапе?

На данном этапе признаки потенциальной компрометации незначительны, и их крайне сложно выявить с помощью средств внутреннего мониторинга. Эффективным инструментом является мониторинг внешних цифровых рисков, с помощью которого можно отследить объявления о покупке/продаже информации или доступа. Крайне важно на этом этапе с помощью организационных мер также минимизировать риски, связанные с рекрутингом работника злоумышленниками и с возможными действиями мотивированных инсайдеров.

Технические меры защиты

Использование систем UEBA/UBA для выявления аномальной активности пользователей. UEBA/UBA позволяют не только обнаружить нетипичную внутреннюю угрозу, но и предотвратить ее на этапе начала аномальных действий или подозрения на совершение неправомерных действий. На практике UEBA/UBA используются как дополнительные модули в решениях DLP (Data Loss Prevention / Data Leak Prevention). Генерируемые отчеты позволяют выявить переработки (что может свидетельствовать о скором «выгорании» работника), нетипичное активное общение с коллегами или увеличение объема переписки с неизвестными третьими лицами.

Мониторинг внешних цифровых рисков (сервис киберразведки) позволяет своевременно обнаружить интерес злоумышленников к ресурсам организации, а также выявить наличие работников, которые уже прошли стадию «переломного момента» и опубликовали в Даркнете или телеграм-каналах объявление с готовностью продавать конфиденциальную информацию.

Организационные меры защиты

Проверка соискателей при приеме. Перед наймом команды необходимо убедиться не только в профпригодности, но и провести проверку кандидатов на благонадежность.

Микроклимат компании. На этом этапе большое значение имеют HR-процессы и инструменты, применяемые в компании. Важно вовремя выявлять нелояльных и неудовлетворенных сотрудников, понимать, какие работники находятся в зоне риска, и предотвращать их потенциальный «переломный момент» путем урегулирования спорных ситуаций.

Выстраивание взаимодействия HR-подразделения, ИТ-подразделения и ИБ-подразделения. Несмотря на превентивные действия со стороны HR, важно также превентивно ограничивать действия потенциально мотивированных инсайдеров. Любые события, связанные с увольнением работников, сокращением штата или применением дисциплинарных взысканий, HR-подразделение должно доводить до сведения ИТ и ИБ. Работники ИТ и ИБ, в свою очередь, должны принимать необходимые меры — усиливать мониторинг за такими работниками, корректировать права доступа.

Предупреждение об ответственности. Хорошей практикой является подписание со всеми работниками и подрядчиками соглашений о неразглашении конфиденциальной информации и соблюдении требований ИБ, предъявляемых компанией. Таким образом фиксируется, что работники и подрядчики понимают степень их ответственности и стремятся воздержаться от нанесения ущерба компании путем разглашения конфиденциальной информации, нарушения работы ресурсов компании и т. д., так как такие согласия имеют юридически значимую силу и ведут к привлечению к ответственности.

Разведка и сбор данных

Чем характеризуется данный этап

Инсайдер проводит активную разведку внутри инфраструктуры — изучает доступные системы, общие файловые ресурсы и папки обмена. Необходимая информация собирается и сохраняется, как правило, локально для дальнейшей эксфильтрации или распространения. Данный этап характерен как для мотивированных инсайдеров, так и для работников, которые любят сохранять информацию «на всякий случай».

Что мы наблюдаем

«Успешность» этапа сбора данных во многом определяется текущими полномочиями работника и зрелостью процесса управления правами доступа к ресурсам.

По опыту проведения экспертных аудитов, у порядка **70%** компаний обнаруживаются критичные недостатки в процессе управления доступом. Например, при отсутствии мер автоматизации и контроля пользователи и администраторы действуют по принципу удобства и оперативности, самостоятельно определяя набор прав, зачастую оставляя его «по умолчанию».

На **83%** проектов по внутреннему пентесту нам удается получить доступ к критичной информации компании с правами обычной учетной записи, не прибегая к повышению привилегий. Такая информация чаще всего встречается на следующих «коммунальных» ресурсах: **файловые хранилища, SharePoint, Confluence и т. д.**

Вторая частая проблема — изначально избыточный набор полномочий работника. С профессиональным ростом и продвижением по карьерной лестнице набор прав усложняется, «временные» права зачастую остаются постоянными. По опыту проведения аудитов, порядка **55%** компаний выстроили системный процесс пересмотра прав доступа, но, как правило, контрольные процедуры ограничиваются блокировкой неиспользуемых учетных записей.

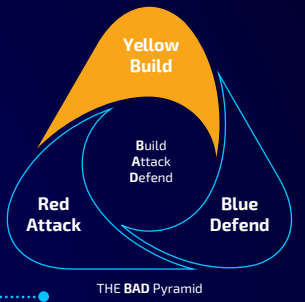
На практике мы наблюдаем, что наиболее высокую опасность представляют работники, которые уже имеют привилегированные учетные записи (администраторы инфраструктуры, работники бизнес-подразделений, для которых обосновано предоставление такого доступа, подрядчики и т. д.). Именно они могут за короткое время нанести наибольший вред компании в силу своих полномочий.

Беспорядок в файловых «шарах», ошибки с правами доступа к каталогам и папкам обмена — системные проблемы, которые мы наблюдаем в рамках проектов по внедрению решений DCAP/DAG и IDM. В отсутствие механизмов автоматической очистки каталогов информация, отправленная на печать/ передаваемая внешним подрядчикам/используемая для совместной работы, с течением времени «забывается» в каталогах, однако не становится менее ценной.

JET SECURITY TEAM

Кейсы

В рамках одного из проектов по внедрению UEBA/UBA в крупной ритейл-компании была выявлена аномальная активность руководителя подразделения, который вскоре должен был покинуть компанию. Дополнительные проверки средствами DLP показали, что он за несколько вечеров сохранил более 18 ГБ информации на свой рабочий стол в папку с названием «secret». Все скопленные там файлы и данные были скопированы из большого количества папок на корпоративном сетевом хранилище, к которым для него был открыт доступ. В ходе детального анализа выяснилось, что доступ сотруднику был предоставлен для выполнения краткосрочной задачи, но не был отозван после ее завершения. Служба ИБ оперативно провела работы по удалению информации из папки пользователя, блокировке избыточных прав доступа как в сетевом хранилище, так и в бизнес-системах, и установила повышенный контроль за деятельностью руководителя в течение оставшегося до увольнения времени.

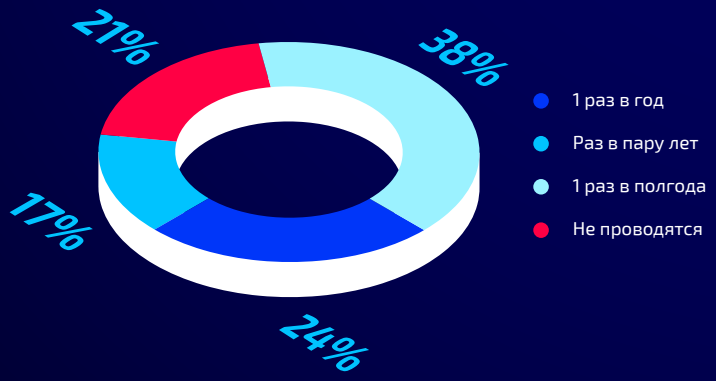


THE **BAD** Pyramid

Результаты опроса

Больше половины компаний **(62%)** на регулярной основе (один раз в полгода-год) осуществляют мероприятия по инвентаризации прав доступа к ресурсам, определенным компаниями как критичные, что подтверждает результаты наших проектных наблюдений. В **21%** компаний инвентаризация прав доступа не осуществляется совсем.

Как часто проводятся мероприятия по инвентаризации прав доступа к критичным ресурсам?

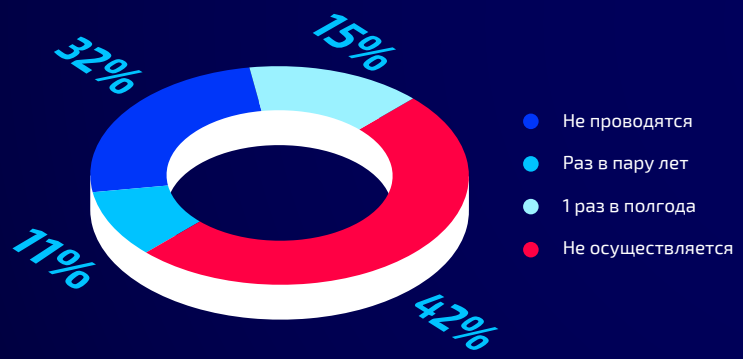


Смена паролей привилегированных учетных записей после увольнения или прекращения работ по договору является самой популярной мерой для защиты от неправомерных действий привилегированных пользователей **(64%)**. Регулярные мероприятия по пересмотру прав привилегированных пользователей проводятся в 47% компаний. При этом компаниями также используются средства автоматизации защиты от действий привилегированных пользователей — системы класса PIM/PAM **(31%)** и DAM **(15%)**

Какие меры применяются для защиты от неправомерных действий привилегированных пользователей?

Мероприятия, направленные на моделирование действий инсайдера путем проведения работ по тестированию на проникновение, осуществляются большинством компаний **(57%)** на регулярной основе (один раз в полгода-год). **32%** компаний указали, что тестирования на проникновение данными методами не осуществляются.

Как часто проводятся тестирования на проникновения методами «серого ящика» и «белого ящика» для определения возможностей злоумышленников?



Как защититься на этом этапе?

На данном этапе меры защиты должны быть направлены на предотвращение несанкционированного доступа к критичной информации и отслеживание аномальной активности пользователей. Одной из основных трудностей на данном этапе является сложность разграничения между легитимной активностью сотрудников компании и действиями инсайдеров, которые проводят разведку. Стоит отметить, что даже небольшие признаки аномального поведения могут оказаться ключевыми, но их выявление требует глубокого анализа и мониторинга.

Организационные меры защиты

Повышение осведомленности пользователей о критичности их аутентификационных данных, необходимости их безопасного хранения. Также важно донести до пользователей риски использования простых паролей и реализовать технические ограничения для создания простых паролей посредством встроенных механизмов компонентов инфраструктуры.

Управление процессом контроля доступа, позволяющим контролировать выдачу прав доступа, соблюдение принципа минимальных привилегий и отслеживание аномальной активности по несанкционированной выдаче повышенных прав доступа.

JET SECURITY TEAM

Технические меры защиты

Использование специализированных **менеджеров паролей**: как минимум — для привилегированных пользователей, как максимум — использование их всеми работниками компании для хранения паролей.

Использование **систем DCAP/DAG**, которые позволяют выполнять централизованный аудит безопасности таких ресурсов, как файловые хранилища, контроллеры домена, почтовые серверы, SharePoint, Confluence, Jira и т. д. DCAP/DAG проводят сканирование подключенных защищаемых ресурсов и аудит операций пользователей. В результате решение определяет избыточные права доступа к данным, детектирует хранение чувствительной информации, фиксирует случаи аномальной активности (например, массовое создание, копирование или уничтожение информации) с возможностью заблокировать дальнейшие действия пользователя с ресурсом.

Использование **IDM-системы** для автоматизированного управления правами доступа. Система является единым и актуальным источником информации о том, какие пользователи, к каким ресурсам и на каком основании имеют доступ. Также система позволяет автоматизировать пересмотр прав доступа, контролировать права доступа всех пользователей и осуществлять своевременную блокировку и отзыв прав уволившихся работников. IDM-системы ощутимо минимизируют риски некорректной выдачи прав доступа и забытых привилегий.

Использование **DAM-систем** для защиты конфиденциальных баз данных. DAM обеспечивает мониторинг доступа к базам данных и фиксацию специфичных действий с ними (обращение к таблицам с критичными данными, запрос большого массива данных от пользователя, ошибки доступа и т. д.).

Использование **систем PIM/PAM** для контроля действий привилегированных пользователей. С помощью этих систем можно осуществлять аудит активностей администраторов и пользователей сети, централизованно управлять аутентификацией и авторизацией пользователей. Также возможна запись сессий привилегированных пользователей, что облегчает расследование инцидентов.

Использование **NTA/NDR** для анализа аномалий корпоративного сетевого трафика. Системой могут быть выявлены такие аномалии, как внутреннее сканирование и передача большого количества информации по сети. Решение осуществляет обнаружение вредоносных программ и запрещенных приложений внутри сети, что актуально, если инсайдер замотивирован совершить неправомерные действия с инфраструктурой компании.

Использование **SIEM-систем**. На данном этапе для мониторинга аномального поведения достаточно интеграции SIEM-системы с перечисленными выше СЗИ, что позволит повысить эффективность мониторинга инцидентов ИБ за счет оперативного реагирования. Также при настройке необходимых правил корреляции система позволяет отслеживать действия по сбору чувствительной информации (например, выгрузку большого объема данных через FTP внутри корпоративного сегмента, выгрузку репликации контроллера домена или баз данных). Для привилегированных пользователей рекомендуется настраивать правила, связанные с разведкой корпоративной сети, а именно: сетевые сканирования, попытки подключения к определенным портам, получение доступа к административным учетным записям и др.

Эксфильтрация / Реализация атаки

Чем характеризуется данный этап

Инсайдер совершает конечные действия, направленные на достижение своих целей, таких как кража/повреждение данных, активов или другие атаки. Украденные данные «выводятся» через печать документов, внешние накопители, передаются на внешние файловые сервисы или отправляются на личную почту. Действия на этапе эксфильтрации типичны как для нелояльных инсайдеров, так и для нарушителей «по незнанию».

Что мы наблюдаем

Основным инструментом для предотвращения кражи данных на этом этапе являются DLP-системы, для которых наиболее распространен контроль именно почтового трафика. При этом наиболее часто «в тени» остаются такие каналы утечки, как веб-трафик, мессенджеры и сервисы внешнего обмена (OneDrive, Google Drive, Яндекс.Диск, DropBox и т. д).

Режим блокировки отправки информации за периметр посредством DLP-систем реализован не более чем в **33%** компаний. Ключевым фактором успеха работы DLP-системы в режиме блокировки является скорость реагирования на события ИБ, и во избежание риска остановки бизнес-процессов необходима дополнительная подготовка и выделение квалифицированных работников для регулярного мониторинга заблокированных сообщений. Однако не все компании готовы к этому из-за ограниченного штата работников ИБ.

Также частой ошибкой является использование только тех политик, которые настроены в системе по умолчанию. Неадаптированные под бизнес-процессы политики выдают большое количество ложных событий. В таких случаях система может использоваться, только когда необходимо провести ретроспективный анализ в рамках сбора информации об инцидентах.

Несмотря на то, что режим коммерческой тайны (далее — КТ) является единственным правовым механизмом для защиты конфиденциальной информации, в последние годы мы наблюдаем низкий интерес к выстраиванию этого режима. Чаще всего меры по защите КТ были предприняты давно и внедрялись в парадигме работы с бумажными носителями. Не все компании перестроили свой подход с учетом работы с электронными документами, требования законодательства выполняются не полностью или создается видимость их выполнения «для галочки». Например, не осуществляется маркировка информации в электронном виде, отсутствуют грифы информации в бизнес-системах, и действительно конфиденциальными в таком случае являются только бумажные носители, на которые работники могут проставить гриф.

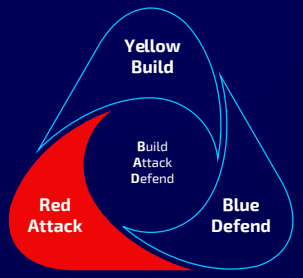
В большинстве компаний отсутствует классификация конфиденциальной информации в зависимости от требований к защите. Работники понимают, что не все документы должны относится к КТ, некоторые из них не столь критичны, однако других классов информации в компании нет. Из-за этого возникают различные ошибки при отнесении информации к КТ — информация защищается либо избыточно, либо недостаточно. Однако типов градации может быть больше, чем установлено российским законодательством (например, «Информация для внутреннего использования», «Информация средней критичности»), и отсутствие критериев ее критичности приводит к тому, что конфиденциальность информации для работников компании остается «серой» зоной без очевидных правил.

Кейсы

Системный администратор компании после своего увольнения воспользовался привилегированной учетной записью, которая не была заблокирована в момент увольнения. Используя расширенные права доступа, бывший администратор нарушил работу серверов, отвечающих за производственную линию и обработку заказов, а также удалил файлы, необходимые для их восстановления. В результате инцидента было остановлено производство, а в центре дистрибуции была прекращена отгрузка товара. Из-за этого компания теряла ежедневно около $100 000 до тех пор, пока работа серверов не была восстановлена.

Работник компании, назначенный руководителем, получил доступ к системе ERP, в которой хранится критичная документация, описание структуры бизнес-процессов, ключевые клиенты, их контакты и пр. Через две недели после получения доступа к данным сотрудник уволился. У компании возникло подозрение на предмет утечки.

Расследование проводила команда Jet CSIRT, при анализе было проработано несколько гипотез, и наиболее вероятной оказалась утечка через программное обеспечение для удаленного администрирования AnyDesk. Было обнаружено значительное количество передаваемой информации с использованием этого ПО (более 4 ГБ), а также подтверждено, что во время работы AnyDesk осуществлялся доступ к конфиденциальным документам, предварительно выгруженным из системы ERP.



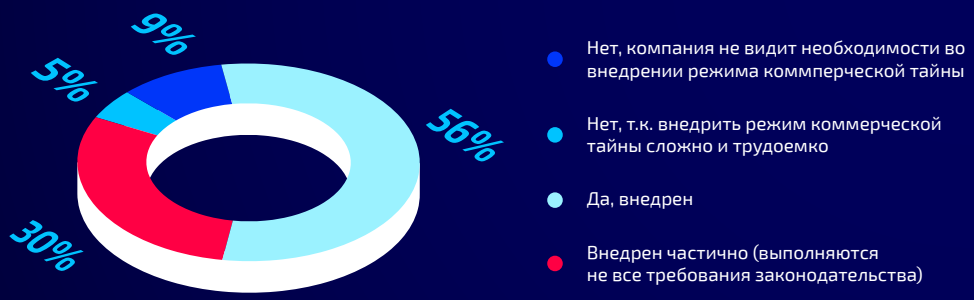
THE **BAD** Pyramid

Результаты опроса

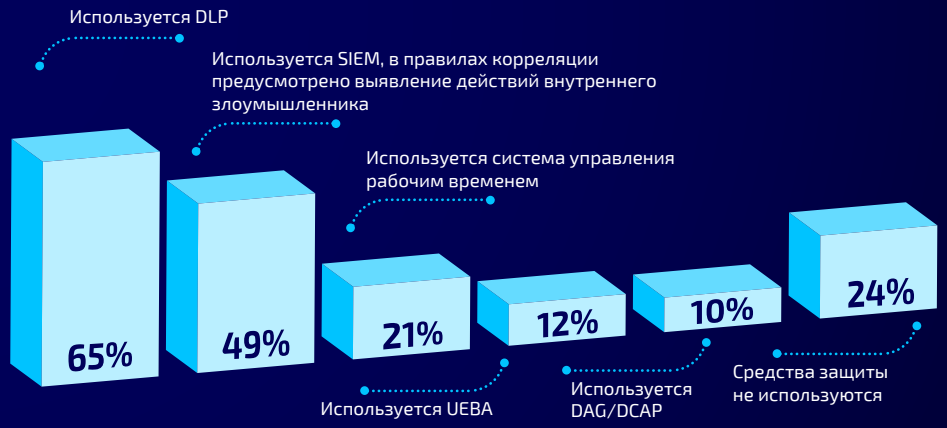
Согласно опросу, у большинства компаний **(56%)** внедрен режим коммерческой тайны (в соответствии с требованиями Федерального закона № 98 «О коммерческой тайне»). При этом **14%** компаний не внедряют режим коммерческой тайны из-за сложности и трудоемкости / отсутствия необходимости во внедрении.

В большинстве компаний в качестве основного средства защиты для выявления и предотвращения действий инсайдеров используются автоматизированные средства — DLP- и SIEM-системы. Только **11%** компаний используют сервисы и услуги киберразведки в качестве дополнительной меры. При этом **24%** опрашиваемых компаний не используют средства защиты от инсайдеров.

Внедрен ли в компании режим коммерческой тайны?



Какие средства защиты используются для выявления инсайдеров?



Для предотвращения несанкционированной передачи конфиденциальной информации за пределы внутреннего периметра в большинстве случаев используется блокировка передачи контента DLP-системой — в основном, конфиденциальной информации **(33%)** и зашифрованных файлов, содержимое которых неизвестно **(25%)**.

В **28%** компаний используются визуальные метки конфиденциальности информации, и в **15%** используются скрытые метки конфиденциальности. При этом в **26%** компаний меры для предотвращения передачи конфиденциальной информации не принимаются.

Какие меры принимаются для защиты конфиденциальной информации от несанкционированной передачи за пределы внутреннего периметра?

JET SECURITY TEAM

Как защититься на этом этапе?

Правовые меры защиты

Выстраивание / корректировка режима защиты КТ и соответствующих процессов. Действующий режим КТ, выстроенный в соответствии с законодательством РФ, обеспечивает компаниям законное основание для отстаивания своих прав в случае необходимости привлечения работников к ответственности.

Организационные меры защиты

Регламентирование процессов обработки и защиты конфиденциальной информации компании и правил допустимого использования.

Повышение осведомленности пользователей, сфокусированное на донесении правил безопасной работы с конфиденциальной информацией и важности их соблюдения.

Технические меры защиты

Для контроля за утечками самым распространенным средством защиты являются системы DLP. Корректное определение типов конфиденциальности и четкое понимание того, какие случаи передачи информации являются легитимными, обеспечивает корректную настройку правил системы и позволяет снизить количество ложных срабатываний.

Маркирование электронных документов позволяет упорядочить работу с конфиденциальной информацией компании. Системы, осуществляющие маркирование электронных документов, решают вопрос маркировки в электронном виде начиная с самого создания документа и повышения осведомленности работников за счет видимых грифов конфиденциальности.

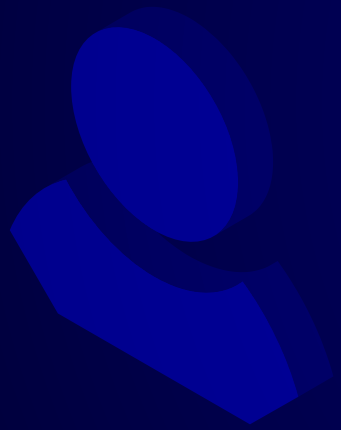
Использование систем VDR для корпоративного защищенного обмена файлами. В случае отсутствия корпоративных систем для обмена данными работники зачастую используют общедоступные облачные сервисы. Использование контролируемых корпоративных сервисов позволяет повысить цифровую гигиену в компании, обеспечить шифрование передаваемых и хранящихся файлов и разграничить доступ ко всем документам, загружаемым на ресурс для конкретных пользователей и третьих лиц.

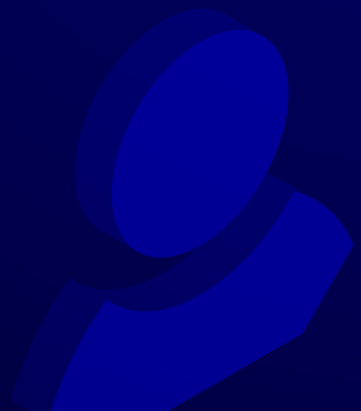
Использование SIEM-систем с настроенными правилами корреляции, которые позволяют выявить инсайдера на этапе сбора данных. На данном этапе правила должны быть направлены на контроль за данными, выгружаемыми за пределы внутреннего периметра, например: подключение неавторизованных съемных носителей у пользователей, находящихся под особым контролем; туннелирование трафика для его маскировки; превышение объема данных, выгружаемых за пределы периметра компании.

Сокрытие следов

Чем характеризуется данный этап

Заметание инсайдером следов — наиболее легкий в отслеживании этап (инсайдер пытается замести следы своих действий, чтобы избежать обнаружения, этот этап отслеживается легче всего относительно остальных). Пытаясь избавиться от доказательств совершения несанкционированных действий (очистка журналов событий, остановка служб, удаление файлов, пользователей и прочих сущностей), инсайдер может «наследить» еще больше.





Что мы наблюдаем

По нашему опыту, инсайдеры задумываются о необходимости сокрытия следов лишь в **13%** случаев, чаще всего расследования происходят как раз по логам, журналам и оставленным «горячим» следам. Мы не фиксировали инциденты с удалением учетных записей, файлов или остановкой служб журналирования в инфраструктурах наших заказчиков.

Инциденты на этапе сокрытия следов при этом эффективно детектируются с помощью правил корреляции SIEM-системы, вот некоторые из них:

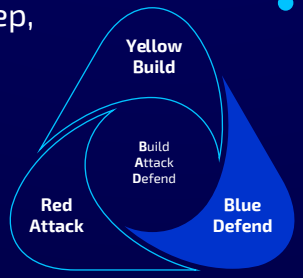
- Изменение политик аудита на Windows/Linux хостах
- Изменение журналов на Windows/Linux хостах
- Очистка журналов Security на узле
- Удаление учетных записей
- Остановка службы журналирования
- Выгрузка чувствительных данных из бизнес-систем
- Нелегитимные/подозрительные действия в бизнес-системах и др.

Такие правила мало подвержены ложноположительным срабатываниям и поэтому позволяют обнаружить нелегитимные действия и потенциального инсайдера, даже если на предыдущих этапах Insider Kill Chain выявить нарушителя не удалось.

Кейсы

Команда Jet CSIRT проводила расследование инцидента в одной из коммерческих организаций. Для управления множеством бизнес-процессов в организации использовалась популярная система SAP, где осуществлялась работа с финансовой информацией компании. Организация обратилась в Jet CSIRT после инцидента с несанкционированным доступом, повлекшим серьезную утечку критической информации, предположительно, из этой системы. Несмотря на низкую зрелость ИБ-процессов в компании, недостаточно грамотную защиту информационных активов, а также назначение и разграничение пользовательских привилегий, в организации осуществлялся постоянный сбор событий с множества хостов в систему мониторинга на базе Open Source решения. SAP имеет собственный аудит, который позволяет отслеживать множество важных с точки зрения ИБ событий, происходящих в приложении. Однако в нашем случае данный аудит не был настроен.

Администратор компании настроил логирование основных журналов на рабочих станциях сотрудников и собрал их в систему мониторинга, что позволило нашим специалистам составить список хостов и пользователей, постоянно использующих приложение. Систему SAP ежедневно посещало более десятка пользователей, однако только на одном хосте, владельцем которого являлся инсайдер, были стерты журналы событий и остановлены службы журналирования, что стало одним из доказательств сокрытия им следов после инцидента.

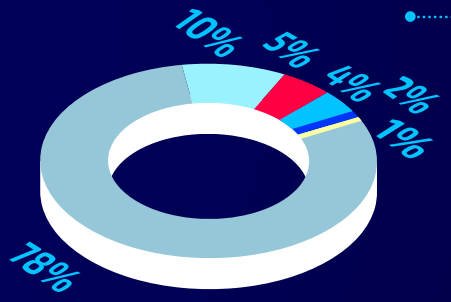


THE **BAD** Pyramid

Результаты опроса

Только **22%** из числа опрошенных компаний сталкивались с инцидентами, связанными с сокрытием следов, за последний год. Самым популярным среди этих инцидентов являлась очистка журналов событий **(10%)**. Инцидентов, связанных с остановкой служб журналирования на хостах, удалением файлов и пользователей, регистрировалось меньше (**5%**, **4%** и **2%** соответственно). При этом инциденты, связанные с физическим уничтожением (например, шредирование конфиденциальных документов), не отслеживаемые техническими средствами, выявлялись только в **1%** случаев.

Какие инциденты, связанные с сокрытием следов, вы выявляли у себя за последний год?



- Очистка журналов событий
- Остановка служб журналирования на хосте
- Удаление файлов, в которых содержится собранная инсайдером информация
- Удаление пользователей (включая недавно созданных)
- Физическое уничтожение доказательств инцидента
- Инциденты, связанные с сокрытием следов, не наблюдались

Как защититься на этом этапе?

Несмотря на то, что сокрытие следов является последним этапом в инсайдерской цепочке, когда инцидент по сути уже случился, важно предусмотреть ряд мер, важных с точки зрения расследования инцидента. При этом стоит учитывать, что избыточно собираемые события могут привести к перегрузке информацией, затрудняя мониторинг и нагружая ограниченные ресурсы системы мониторинга. С другой стороны, недостаточная настройка аудита может привести к упущению критически важных индикаторов компрометации.

Организационные меры защиты

Определение необходимых для журналирования событий с точки зрения информационной безопасности и **контроль за осуществлением журналирования**. События, подлежащие журналированию, должны быть определены как минимум для критичных ресурсов компании. Зачастую события, журналируемые системами по умолчанию, не позволяют увидеть всей картины при расследовании инцидента. В связи с этим необходимо определить необходимые параметры журналирования для хостов в зависимости от их роли (рабочие станции, серверы, контроллеры домена, бизнес-системы) и осуществлять настройку в соответствии с ними.

Технические меры защиты

Сбор событий информационной безопасности в единую **LM/SIEM**-систему для их хранения, обработки, нормализации и корреляции. Важно предусмотреть непрерывную отправку событий в единое хранилище. Таким образом, даже если пользователь имеет достаточно высокие привилегии, чтобы попробовать скрыть следы своих действий, события об этом всё равно останутся в хранилище и послужат доказательством в дальнейшем расследовании. Даже простые Open Source продукты, такие как стек ELK, порой являются крайне полезными при проведении постинцидентной активности.

На критичные хосты рекомендуется устанавливать **дополнительные средства мониторинга** (такие как Sysmon для Windows). Стандартные события в Linux также малоинформативны, поэтому рекомендуется использовать решения, предоставляющие расширенные возможности аудита, такие как auditd, auditbeat, eBPF. В бизнес-системах, обеспечивающих самые важные процессы компании (таких как ERP (Enterprise Resource Planning), CRM (Custore Relations Management), WFM (Workforce Management)), сбор событий является наиболее важным. В некоторых случаях может потребоваться дополнительная работа по настройке их аудита и нормализации событий для их корректной обработки SIEM- и LM-системами.

Использование **SIEM-системы** и настройка правил корреляции. В случае обеспечения сбора достаточно полного перечня событий необходимо использование SIEM-систем, позволяющих на основе большого объема данных выявить взаимосвязи между событиями и предотвратить реализацию инцидента. SIEM-системы работают на основе правил корреляции, при корректной настройке которых их можно использовать для выявления подозрительной активности. Например, это могут быть события очистки журналов событий, остановки или удаления служб, файлов, блокировки пользователей. Очень простой пример — настройте правило, которое будет следить за появлением события 1102 («журнал аудита был очищен»). Оно появляется автоматически каждый раз, когда происходит очистка журнала Security.

Выводы

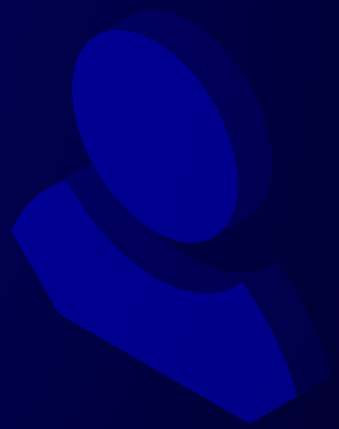
Современные системы безопасности часто проектируются в парадигме доверия к тем или иным лицам (например, доверие к собственным работникам, третьим лицам, контрагентам и т. д.). Особенности эксплуатации доверия к третьим лицам мы подробно рассмотрели в предыдущем аналитическом отчете **«Атаки на подрядчиков: эксплуатация доверия».**

В то же время инсайдерские угрозы могут привести к не менее серьезным последствиям для организаций всех размеров и всех секторов бизнеса. Часто компании не рассматривают внутренних нарушителей всерьез, безоговорочно доверяя своим работникам. Такое доверие предоставляет возможности для злоупотребления со стороны рядовых сотрудников, поэтому корректное выстраивание обнаружения и предотвращения инсайдерских угроз является одной из актуальных проблем кибербезопасности.

Несмотря на то, что методы инсайдеров могут варьироваться, основные атаки, как правило, происходят через ряд последовательных этапов «инсайдерской цепочки» **(Insider Kill Chain)**:

- Рекрутинг / Переломный момент
- Разведка и сбор данных
- Эксфильтрация / Реализация атаки
- Сокрытие следов

Внедрение мер контроля, приведенных в разделах настоящего отчета, на каждом из четырех этапов поможет повысить эффективность предотвращения, обнаружения таких внутренних угроз и своевременного реагирования на них.



Предыдущие аналитические отчеты по информационной безопасности

О нас

Центр информационной безопасности компании **«Инфосистемы Джет»** — профессиональное сообщество специалистов по ИБ.

Мы защищаем коммерческие компании и государственные организации от киберугроз уже более 25 лет. Сегодня наша команда — это более 450 экспертов в области информационной безопасности, которые реализуют порядка 300 комплексных проектов в год
для защиты бизнеса от киберугроз в России и СНГ.

Наша главная задача — создание и внедрение систем, обеспечивающих реальную безопасность бизнеса.

О компании

«Инфосистемы Джет» — одна из крупнейших ИТ-компаний в России. С 1991 года работает на рынке системной интеграции, реализуя ежегодно **более 1000 проектов**, многие из которых уникальны по масштабу и сложности. Штат — более 2000 сотрудников.

Компания располагает несколькими офисами и представительствами в России. Входит в ТОП-5 крупнейших российских ИТ-компаний (RAEX 2023г.). Лидер на рынке ИТ-аутсорсинга в России (Tadviser 2022г.), **№1** среди крупнейших поставщиков инфраструктуры дата-центров (Cnews 2022г.), **№2** среди крупнейших поставщиков ИТ-услуг (RAEX 2023г.), **№2** среди крупнейших интеграторов в сфере защиты информации (CNews Analytics, 2022г.), №2 среди крупнейших поставщиков для промышленности (Tadviser 2022г.), **№2** среди крупнейших поставщиков для российских банков (Tadviser 2022г.).

Ключевые направления деятельности: ИТ-инфраструктура, сети и инженерные системы, ИТ-аутсорсинг, информационная безопасность, машинное обучение, заказная разработка ПО, внедрение и сопровождение бизнес-приложений enterprise-уровня, промышленная безопасность и IoT.