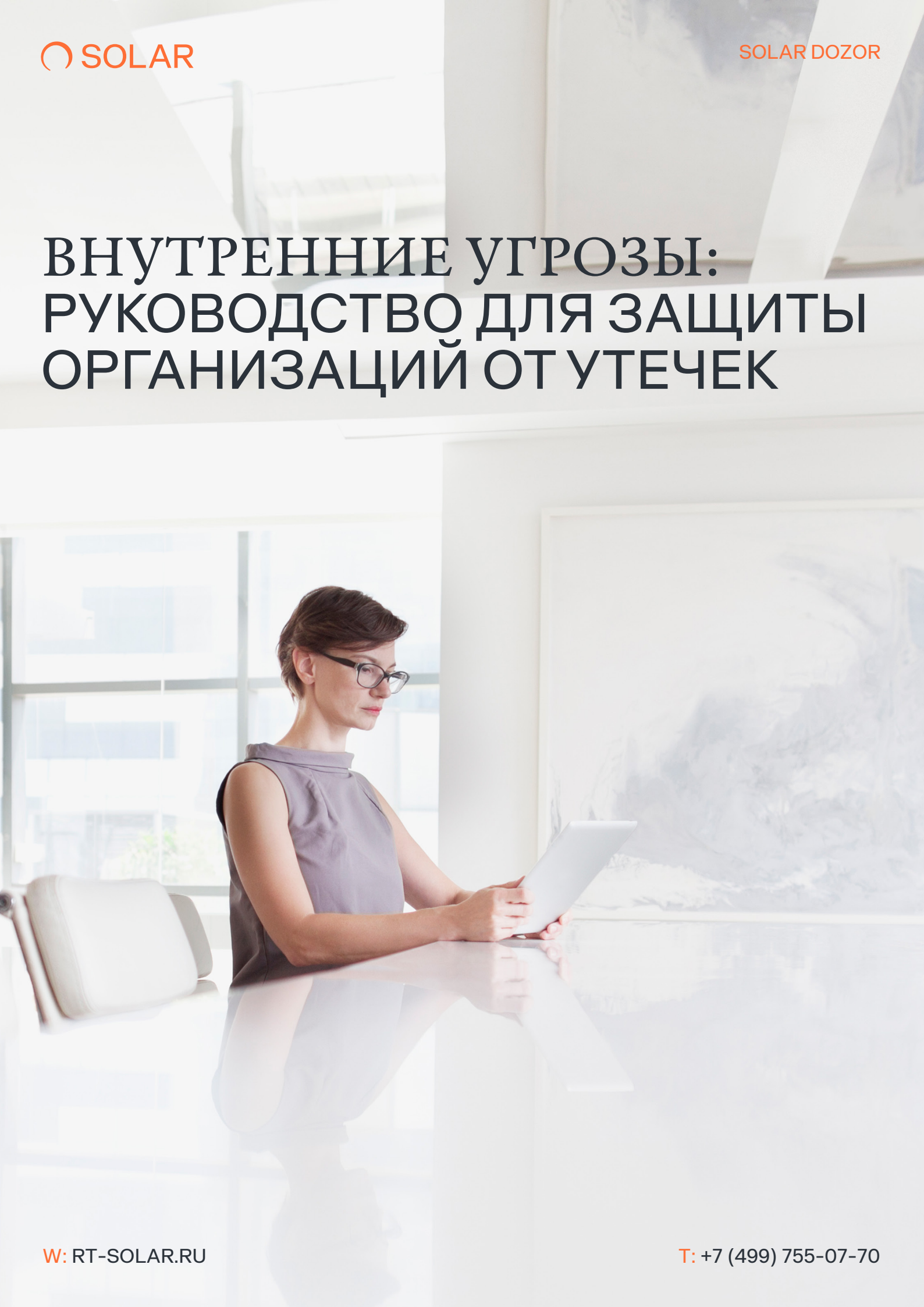
SOLAR

SOLAR DOZOR

ВНУТРЕННИЕ УГРОЗЫ: РУКОВОДСТВО ДЛЯ ЗАЩИТЫ ОРГАНИЗАЦИЙ ОТ УТЕЧЕК



W: RT-SOLAR.RU

T: +7 (499) 755-07-70

Компаниям следует уделять пристальное внимание рискам, которые могут исходить от внутренних пользователей

55%

Инциденты, связанные с халатностью

25%

Инциденты, связанные с преступными инсайдерами

20%

Инциденты, связанные с кражей учетных данных пользователей*

Когда дело доходит до угроз безопасности компаний и борьбы с утечками данных, всеобщей огласке, как правило, придаются внешние угрозы, они привлекают к себе гораздо больше внимания, чем внутренние угрозы, хотя число последних из-за злонамеренных или непреднамеренных действий сотрудников растет с каждым годом (60% в 2020 году, 67% в 2022 году, 71% в 2023 году)*.

Подавляющее большинство организаций (74%) чувствуют себя уязвимыми перед внутренними угрозами, а 83% хотя бы раз столкнулись с утечкой информации по вине инсайдера. 74% организаций отмечают, что инсайдерские атаки стали более частыми за последние 12 месяцев**.

Эти данные свидетельствуют о том, что риск внутренних угроз продолжает расти. А это значит, что необходимо внедрять эффективные меры по борьбе с внутренними угрозами.

*Данные: 2023 Cost of Insider Risks Global Report
** Данные: 2023 Insider Threat Report

Внутренняя угроза, или инсайдерский риск — это угроза, в результате которой интеллектуальная собственность, конфиденциальные и ценные данные могут быть раскрыты пользователями, имеющими легитимный доступ к сети, приложениям или базам данных.

16,2 МЛН ДОЛЛ.

Общая среднегодовая стоимость инсайдерского риска по всему миру*

* Данные: 2023 Cost of Insider Risks Global Report

ТИПЫ ВНУТРЕННИХ ЗЛОУМЫШЛЕННИКОВ

ВРЕДОНОСНЫЙ

Инсайдер, который
стремится причинить вред

- Шпионаж
- Несанкционированное разглашение
- Коррупция
- Саботаж
- Мошенничество
- Служебное преступление

НЕЗЛОНАМЕРЕННЫЙ

Инсайдер, который
не стремится причинить вред

Небрежный инсайдер причиняет вред из-за невнимательности

Теряет USB с важной информацией, оставляет пароль на видном месте, не соблюдает правила по безопасности данных

Ошибочный инсайдер причиняет вред в результате ошибки

Нажимает неправильную кнопку в стрессовой обстановке, ошибочно отправляет электронное письмо неправильному адресату

Обманутый инсайдер причиняет вред в результате того, что его обманули, обхитрили

Сотрудник получает сообщение, которое он принимает за письмо от своего руководителя. Этот адрес злоумышленник подделал, и сотрудник передает ему конфиденциальную информацию

КАК ВНУТРЕННИЕ УГРОЗЫ МОГУТ ПОВЛИЯТЬ НА ВАШ БИЗНЕС?

С каждым днем угрозы кибербезопасности становятся все более сложными, а безопасность данных — еще более хрупкой. Инциденты с участием инсайдеров ежегодно обходятся компаниям в миллионы долларов и могут негативно повлиять на их финансовую состоятельность, а также на репутацию. Кроме того, такие инциденты являются одними из самых опасных рисков в финансовом плане.

С точки зрения защиты не имеет значения, является ли потеря данных результатом атаки внешнего злоумышленника или действий сотрудника. Ваши критически важные данные должны быть защищены независимо от того, кто получает к ним доступ.

701 500 $

Средняя стоимость инцидентов, происходящих по вине злонамеренных инсайдеров

505 113 $

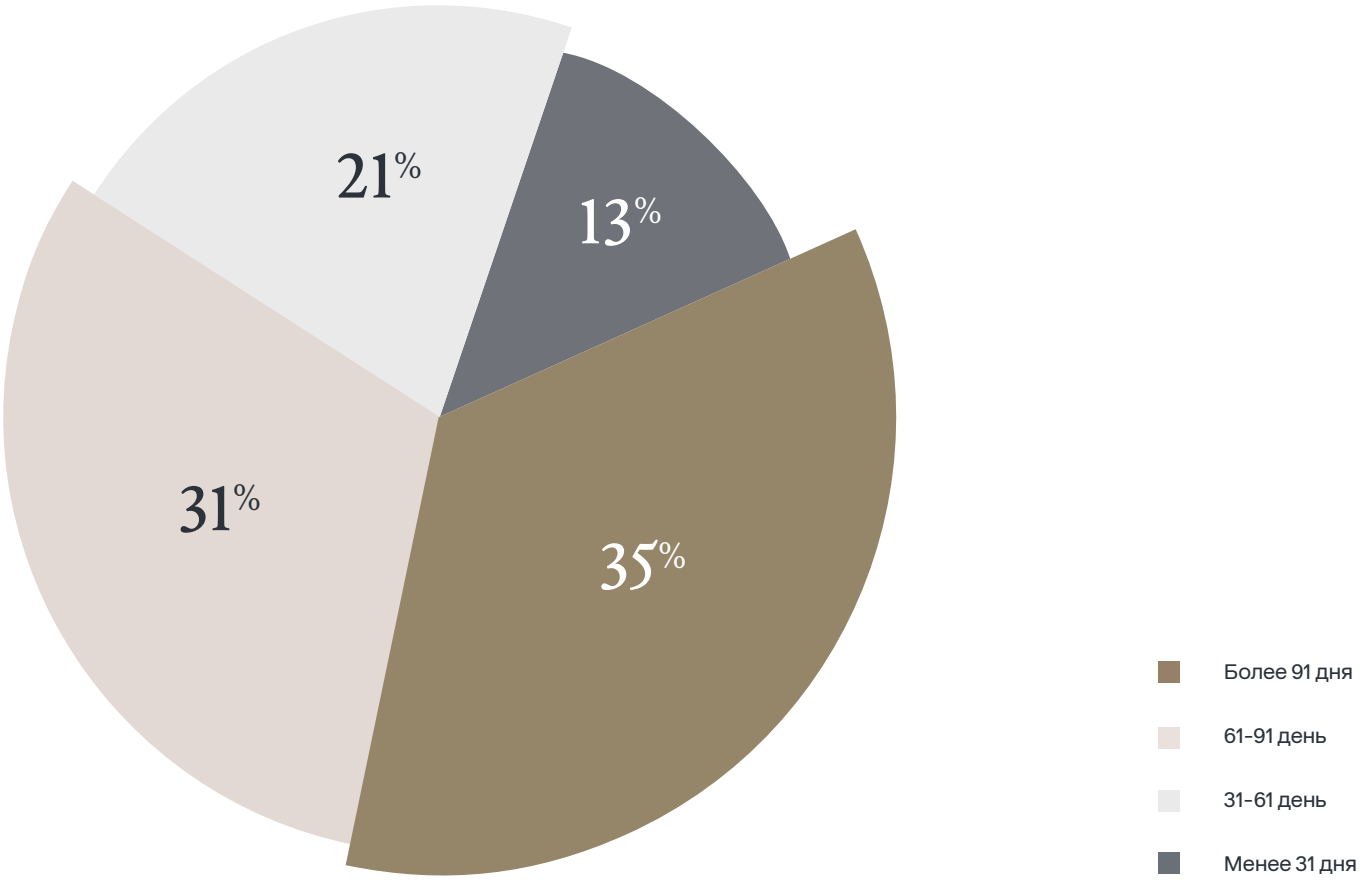
Средняя стоимость инцидентов, происходящих по вине небрежных сотрудников

679 621 $

Средняя стоимость инцидентов, происходящих по вине обманутых инсайдеров*

* Данные: 2023 Cost of Insider Risks Global Report

ПОЧЕМУ ВНУТРЕННИЕ УГРОЗЫ ТАК ОПАСНЫ?



Выявить внутренние угрозы бывает непросто, так как инсайдер имеет законный доступ к информации компании, также он знаком со структурой данных. Более того, он может знать, как защищена эта информация, что существенно облегчает ему обход мер безопасности.

86 ДНЕЙ

В среднем тратят компании на локализацию одного инцидента внутренней безопасности*

* Данные: 2023 Cost of Insider Risks Global Report

ОСОБЕННОСТИ ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ

Для борьбы с внутренними угрозами первоначально следует провести оценку потенциальных рисков, которые могут исходить от инсайдеров.

НЕОБХОДИМО ОПРЕДЕЛИТЬ:

1 Инструменты и способы, используемые инсайдерами

2 Мотивы внутренних злоумышленников

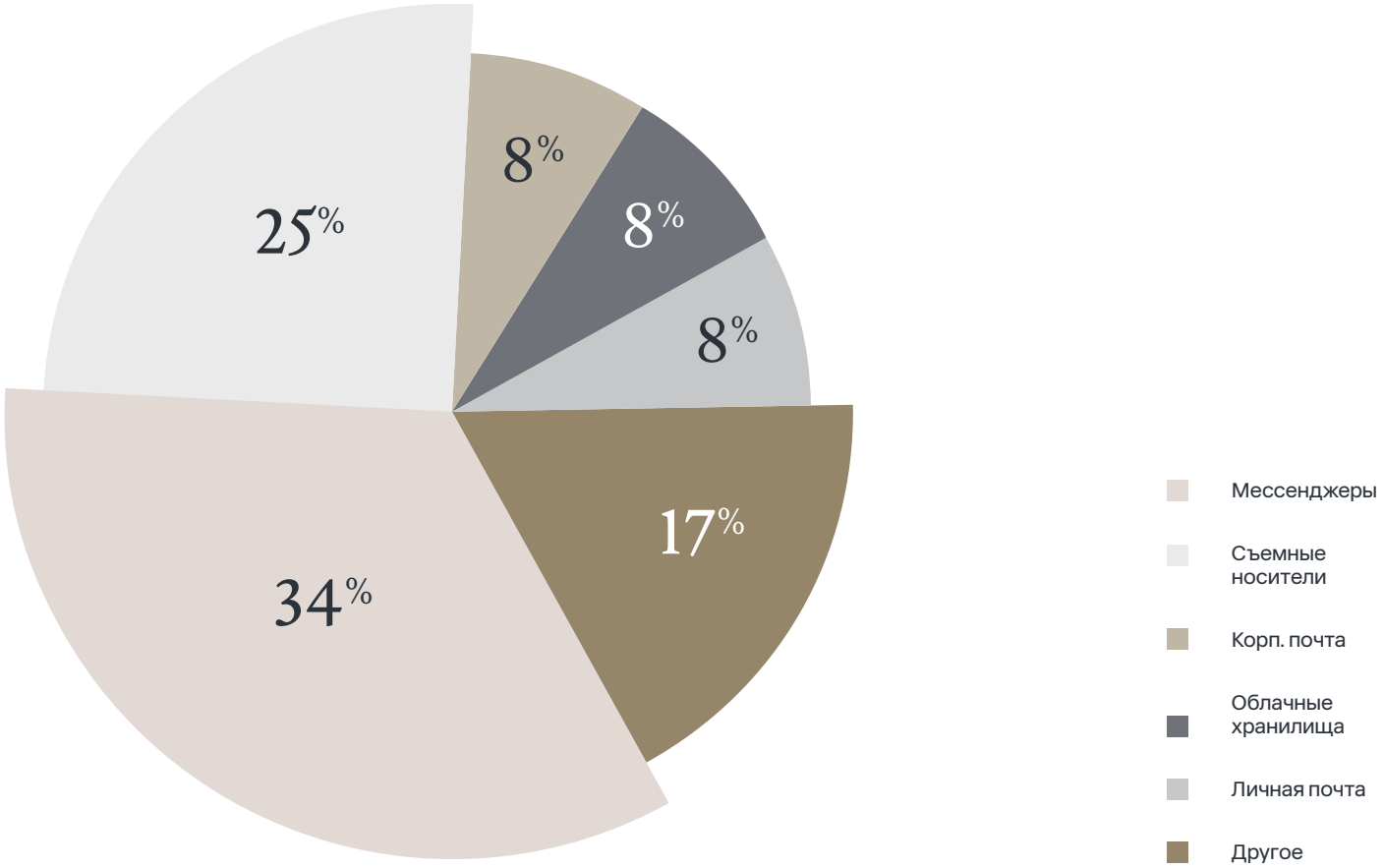
3 Признаки внутренних угроз

ИНСТРУМЕНТЫ И СПОСОБЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ УТЕЧКИ ДАННЫХ

Использование мессенджеров для обмена короткими сообщениями по работе многие считают очень удобным инструментом, так как через них можно передавать текстовые и голосовые сообщения, файлы и видео. Но мессенджеры, как и любые другие электронные средства коммуникации, могут обладать уязвимостями с точки зрения возможных утечек.

Согласно данным исследования ГК «Солар», более 33% мошеннических схем реализуется через мессенджеры, 25% — через съемные носители и 8% — через облачные хранилища, личную и корпоративную почту соответственно*.

КАНАЛЫ РЕАЛИЗАЦИИ МОШЕННИЧЕСКИХ СХЕМ



* Данные: Исследование «Мошенничество и слив данных в российских организациях»

МОТИВЫ ВНУТРЕННИХ ЗЛОУМЫШЛЕННИКОВ

Наблюдение за аномальной активностью на уровне сети может помочь выявить внутренний риск. Если сотрудник выглядит недовольным или затаил обиду, или он начинает выполнять больше задач с чрезмерным энтузиазмом, это может указывать на злонамеренную деятельность.

Основными мотивами для инсайдерских угроз являются: финансовая выгода, ущерб репутации или карьерные амбиции..

ПРИЗНАКИ ВНУТРЕННИХ УГРОЗ

Почему участились случаи инсайдерских инцидентов?

Существует множество причин, по которым количество инцидентов, связанных с внутренними угрозами, увеличивается. Широкая популярность облачных сервисов и концепции «принеси свое устройство» (BYOD) способствует росту числа внутренних угроз.

К тому же пандемия ускорила процесс перехода к удаленному и гибридному формату работы и способствовала распространению как облачных инструментов для совместной работы и хранения файлов, так и теневых ИТ, то есть программного обеспечения, не одобренного организацией. Как следствие, все большему числу сотрудников предоставляется расширенный доступ к сети.

Все это приводит к общей нехватке контроля, что в итоге увеличивает возможности злонамеренных инсайдеров остаться незамеченными системами безопасности.

ПРИЗНАКИ ТОГО, ЧТО КОМПАНИЯ ПОД УГРОЗОЙ

01

Сотрудники не знают, какие шаги они должны предпринимать для обеспечения безопасности используемых ими устройств — как выданных компанией, так и личных (BYOD).

02

Сотрудники нарушают политику безопасности организации для упрощения задач.

03

Сотрудники отправляют конфиденциальные данные в незащищенное облако, подвергая организацию риску.

04

Электронные письма, содержащие конфиденциальные данные, отправляются третьей стороне.

05

Дистанционный доступ к сети и данным в нерабочее время.

06

Многочисленные попытки доступа к заблокированным веб-сайтам.

07

Попытки доступа к USB-портам и устройствам.

08

Частые запросы на доступ к данным, не связанным с должностными обязанностями сотрудника.

09

Вход в систему с различных IP-адресов за короткое время.

Инсайдеры могут действовать тихо, незаметно и потенциально нанести больший ущерб, чем внешние злоумышленники, потому что они уже имеют определенную степень доверительного доступа и прямое представление о «главных сокровищах» организации.

КАКОЕ ЕСТЬ РЕШЕНИЕ?

[01] Определите, какая информация является конфиденциальной и важной для компании

Прежде чем защищать данные от внутренних угроз, необходимо ответить на следующие вопросы:

- Какая информация является конфиденциальной и критически важной?
- Где находится эта информация?
- Кто и какой уровень доступа имеет к этой информации?
- Соответствуют ли текущие меры защиты допустимому уровню риска?

[02] Введите режим коммерческой тайны на предприятии

Необходимо разработать положение о коммерческой тайне и указать перечень конфиденциальных сведений, порядок их учета, хранения и использования. Получите от сотрудников письменное обязательство о неразглашении коммерческой тайны.

[03] Осуществляйте мониторинг доступа к данным, их перемещения и активности пользователей

Управляя правами доступа сотрудников и их обращением с конфиденциальными данными, ограничивая бесконтрольную передачу информации на съемные носители, можно снизить риски утечки. Определите перечень лиц, имеющих доступ к коммерческой тайне, и регламентируйте порядок доступа к этим сведениям.

[04] Обучайте своих сотрудников и составьте для них памятку об ответственности за разглашение коммерческой тайны

Проводите регулярные тренинги по работе с конфиденциальной информацией.

[05] Используйте шифрование данных

Шифрование защищает данные, отправляемые через разные каналы коммуникации (почта, флешки, мессенджеры), от утечки.

[06] Защитите конечные устройства от потери данных

Внедряйте методы борьбы с внутренними рисками. Пользователи могут подключать к сети различные конечные устройства, такие как смартфоны, ноутбуки и принтеры. Усовершенствуйте свою программу кибербезопасности, используя подход к защите данных, основанный на принципе «нулевого доверия» (Zero Trust).

[07] Используйте дополнительные средства защиты данных и классы решений

- Средство предотвращения утечек данных — DLP-система
- Контроль и управление доступом к неструктурированным данным (DCAP-системы)
- Управление учетными записями и правами доступа (IdM, IGA)
- Контроль привилегированных пользователей (PAM)
- Технология единого входа (SSO, Web SSO)
- Антифрод-системы
- Технологии мониторинга обращений к базам данных и бизнес-приложений (DAM-системы)
- Технологии контроля данных в облачных сервисах (Cloud Access Security Broker, CASB)
- Технологии маркировки конфиденциальных данных
- Технологии в области мультифакторной аутентификации (MFA)
- Технологии управления мобильными устройствами и приложениями (Enterprise Mobility Management, EMM)
- Технологии шифрования данных на конечных устройствах пользователей и т. д.

МОНИТОРИНГ И ПРЕДОТВРАЩЕНИЕ ВНУТРЕННИХ УГРОЗ С ПОМОЩЬЮ DLP-СИСТЕМЫ SOLAR DOZOR

Solar Dozor – система для предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP) корпоративного класса. Ее возможности обеспечивают контроль коммуникаций сотрудников, блокировку или изменение нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований.

Кроме этого, Solar Dozor может анализировать поведение пользователей (User Behavior Analytics), что позволяет выявлять аномалии поведения, круг общения и приватные контакты сотрудников, а также профилировать их на основе 20 устойчивых паттернов поведения. Это дает возможность заниматься профилактикой инцидентов безопасности.

В Solar Dozor реализована современная концепция обеспечения внутренней безопасности организации — People-Centric Security. Она предполагает концентрацию внимания службы безопасности на главном источнике угроз — человеке: его фактической роли в коллективе, характере коммуникаций, особенностях работы с защищаемой информацией.

УЗНАТЬ ПОДРОБНЕЕ

SOLAR

W: RT-SOLAR.RU
W: RT.RU

+7 (499) 755-07-70
solar@rt-solar.ru

Центральный офис, 125009,
Москва, Никитский переулок, 7с1