ИССЛЕДОВАНИЕ КОМПАНИИ SEARCHINFORM

# ГДЕ СОЛОМКУ СТЕЛИТЬ: КАК НАХОДИТЬ И ЧЕГО ЖДАТЬ ОТ СОТРУДНИКОВ ГРУПП РИСКА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – это не точная наука вроде математики. Но опыт, скопленный поколениями ИБ-специалистов, позволяет существенно облегчить жизнь в работе с инцидентами. А чтобы не просто выявлять, но и предупреждать нарушения, важно обращать внимание на сигналы о потенциальной опасности. В этом материале мы собрали «коллективное знание» наших клиентов о том, на какие группы риска сотрудников ИБ-службы обращают внимание, почему и как обнаруживают в коллективе с помощью ИБ-программ.

| ГРУППА РИСКА | УГРОЗА: НА ЧТО МОЖЕТ ПОЙТИ СОТРУДНИК | КАК ОБНАРУЖИТЬ СОТРУДНИКА ГРУППЫ РИСКА |
|---|---|---|
| Сотрудник недоволен зарплатой | Слив, «пробив» данных с целью продажи.<br>Откаты, махинации, подделка документов для завышения показателей, незаконного получения бонусов и премий.<br>Саботаж. | Обращайте внимание на обсуждение нехватки денег, низких доходов, чужих зарплат и премий. В DLP («СёрчИнформ КИБ») настройте словарь денежной тематики.<br>Мотивированность на деньги в сочетании с высокими амбициями может быть важным признаком. В линейке «СёрчИнформ» такие факты умеет выявлять программа профилирования сотрудников ProfileCenter. В ней нужно обратить внимание на лидеров рейтинга «Мотивированные на деньги», амбиции 4-5 пунктов. |
| Сотрудник в конфликте с руководством / недоволен задачами / коллегами | Слив данных «из мести», при увольнении; разглашение информации в СМИ и соцсетях.<br>«Подставы» коллег, мошеннические схемы из мотивации «имею право».<br>Распространение негатива в коллективе, «забастовки». | В DLP ищите упоминания руководства (по именам, прозвищам, официальным и неофициальным названиям должностей – «босс», «шеф», «главный») + выражения из словаря мата.<br>Важный признак – демотивированность, в ProfileCenter можно отследить ТОП-лист сотрудников в соответствующем рейтинге. |
| Сотрудник стал работать менее эффективно / нарушает трудовую дисциплину | Побочная деятельность / собственный бизнес / в ущерб работодателю.<br>Саботаж: умышленное растягивание сроков исполнения задач в ущерб репутации компании, увольнение с попыткой исказить/удалить критичные данные. | Обращайте внимание на продуктивность сотрудников. В «СёрчИнформ КИБ» видно по отчетам эффективности и продуктивности, анализируйте переписки тех, у кого самые низкие показатели.<br>Опасное сочетание демотивированности и выходящих за нормальные показатели амбициозности (высокие и низкие) – можно видеть в отчете по рейтингам в ProfileCenter. |
| Сотрудник готовится к увольнению | Вынос «наработок» на новое место работы. Трудоустройство к конкурентам.<br>Распространение негатива в коллективе, «компромата» в СМИ и соцсетях.<br>Внедрение вирусов, заказ взломов, искажение / удаление информации в базах компании из мести. | Контролируйте появление файлов резюме (показывает DCAP-система «СёрчИнформ FileAuditor»).<br>Отслеживайте активность на сайтах вакансий, отправку резюме, общение с рекрутерами. Настройте словарь «поиск работы» в DLP.<br>Обращайте внимание на снижение мотивированности – в ProfileCenter. |

SEARCHINFORM
INFORMATION SECURITY

| ГРУППА РИСКА | УГРОЗА: НА ЧТО МОЖЕТ ПОЙТИ СОТРУДНИК | КАК ОБНАРУЖИТЬ СОТРУДНИКА ГРУППЫ РИСКА |
|---|---|---|
| У сотрудника собственный бизнес/ подработка | Слив ноу-хау, маркетинговых планов, клиентских баз для собственных нужд.<br>Проведение закупок в ущерб компании, переманивание клиентов; использование ресурсов и наработок работодателя в пользу собственного бизнеса. | Обращайте внимание на договоры, счета и т. п. документы с названием сторонних компаний – видно в FileAuditor.<br>Отслеживайте использование сотрудниками email со сторонним почтовым доменом, а также использование в подписи названия других компаний. |
| У сотрудника есть долги и опасные пристрастия (наркотики, алкоголизм, азартные игры) | Слив, «пробив» данных с целью продажи.<br>Работа на конкурентов из-за угроз разоблачения или с целью вознаграждения для решения финансовых проблем.<br>Проведение мошеннических схем в пользу кредиторов либо по собственной инициативе для наживы. | Любые признаки финансовых проблем, активный интерес к алкоголю, наркотикам и пр. – тревожный сигнал для ИБ. Также отслеживайте признаки шантажа и угроз сотрудникам, поступающих от внешних контактов. В DLP можно видеть по словарям соответствующих тематик. |
| Сотрудник использует ПО, которое не требуется по работе (программы удаленного доступа, фоторедакторы и т. п.) | Предоставление доступа мошенникам извне.<br>Подработка в рабочее время.<br>Использование ПО для кражи информации / попыток «незаметно» слить информацию.<br>Использование программ для подделки документов (печатей, подписей), запуск программ для перехвата/взлома паролей и т. д. | Обращайте внимание на загрузку, запуск любого ПО, не относящегося к рабочей деятельности. Особенно программ удаленного доступа, программ по подбору паролей. В DLP видно по соответствующим отчетам. |
| Сотрудник общается с уволенными коллегами | Случайный или намеренный слив данных по дружбе.<br>Снижение лояльности из-за наговоров экс-коллег.<br>Откаты, передача клиентов «за процент», махинации при закупках в пользу экс-коллеги. | Важно знать о контактах с бывшими сотрудниками. Информацию о коммуникациях удобно смотреть в карточках пользователей в DLP, а также по графу связей. Отслеживайте переписки с внешними контактами на рабочие темы по настроенным в DLP «алертам». |
| Сотрудник ведет себя халатно | Слив данных по халатности, случайные отправки критичной информации «не на тот адрес», в избыточном объеме и пр.<br>Случайная компрометация доступов; случайная передача данных злоумышленникам; совершает ошибки и скрывает их. | Составляйте топ «случайных» нарушителей – в DLP можно собирать такую статистику нарушений.<br>DLP отслеживайте пересылку спама коллегам. |
| Сотрудник подвержен социальной инженерии | Переход по зараженным ссылкам, загрузка вирусов, передача информации, платежных данных, доступов к системам. | Обращайте внимание на риск «подверженность чужому влиянию» в профилях пользователей – это можно видеть в ProfileCenter. |
| Сотрудник хранит или имеет доступ к документам, которые не нужны по прямым обязанностям | Умышленная кража данных или слив из-за непонимания их ценности.<br>Умышленное искажение / удаление данных в папках общего доступа, подделка документов на основе имеющихся образцов. | Отслеживайте права доступа, хранение, операции с файлами, которые нужны сотрудникам по работе (анализ по контенту делают DCAP-системы, в частности «СёрчИнформ FileAuditor»).<br>Следите за доступом сотрудников к базам данных и выгрузкам критичной информации. |
| Сотрудник придерживается радикальных убеждений | Продвижение собственной идеологии или стремлении наказать тех, кто продвижению такой идеологии мешает. | Обращайте внимание на интерес и обсуждение сотрудниками религиозных, политических тем. В DLP настройте словари по терминологии, в отчетах о времени на сайтах отслеживайте регулярные посещения тематических сайтов, групп в соцсетях. |

**Сохраните таблицу или скачайте полные данные о карте рисков:**