# В контуре телекоммуникационной безопасности

**Дмитрий Бондарь,**
*директор департамента развития продуктов управления доступом ГК «Солар»*

Киберрискам сейчас подвержены все отрасли российской экономики, однако телекоммуникационная индустрия входит в число наиболее атакуемых. Чаще всего телеком-компании сталкиваются с целенаправленными DDoS-атаками, вредоносным ПО и атаками с использованием социальной инженерии. При этом более половины расследованных атак в 2024 г. были связаны именно со шпионажем, в 2023-м его доля составляла 37%. Что можно противопоставить злоумышленникам, в каких решениях для защиты, в частности персональных данных, заинтересованы операторы?

Одной из примет последнего времени стало снижение продолжительности при увеличении мощности DDoS-атак. Злоумышленники прилагают максимум усилий, чтобы избежать обнаружения и наиболее рационально использовать свои ресурсы для причинения предельно возможного ущерба. В этом же ряду ставка на проведение мультивекторных DDoS-атак, интерес к нанесению вреда предприятиям среднего и малого бизнеса. В частности, по некоторым данным, количество DDoS-атак на предприятия в Поволжье по сравнению с первой половиной 2023 г. возросло в шесть раз.

Не сдает своих позиций вектор социальной инженерии. Утечки персональных и других данных из служб доставки, фармацевтических и медицинских организаций, телеком-компаний позволили злоумышленникам собрать внушительное досье российских пользователей. И этого вполне достаточно, чтобы почти каждая попытка социальной инженерии становилась результативной, причиняла гражданам моральный и финансовый вред.

## Векторы атак на инфраструктуру

Ранее в рамках проектов по анализу защищенности операторов связи, промышленных, энергетических и нефтегазовых компаний специалисты Solar 4RAYS выявили, что 22% уязвимостей веб- и мобильных приложений с высоким уровнем критичности сосредоточены в телекоммуникациях. 36% общего числа уязвимостей в промышленности, ТЭК и энергетике свойственны именно телеком-сегменту.

Для успешных попыток захвата инфраструктуры хакеры чаще всего пользуются несвоевременным обновлением программного обеспечения, что зачастую допускается операторами, слабой парольной политикой компаний и недостатками контроля доступа. Так, в 2024 г. в половине случаев удачных кибератак злоумышленники использовали скомпрометированные аккаунты сотрудников и взломанные учетные записи подрядчиков и субподрядчиков (supple chain и trusted relationship), имеющих доступ к информационным системам компаний, прежде всего крупных организаций.

Количество атак через подрядчиков увеличивается на протяжении последних пяти лет. Но в последнее время это едва ли не ежедневная проблема для многих организаций и предприятий. По оценкам экспертов, примерно 40–50% инцидентов, которые заканчиваются успешными взломами, реализуются через этот вектор.

В 2025 г. эксперты прогнозируют, что увеличится количество инцидентов, связанных с кражей конфиденциальных корпоративных данных, перехватом ключевых сервисов, уничтожением инфраструктуры, взломом подрядчиков для доступа к целевым сетям.

## Слабое звено

Эксперты Solar inRights (IdM-система ГК «Солар») выяснили,

какие факторы в управлении доступом к инфраструктуре способствуют эксплуатации подобных векторов атак. Для этого было проведено исследование, в котором приняли участие руководители, специалисты по информационной безопасности и информационных технологий более 100 крупных организаций, представляющих финансовый, промышленный сегменты, энергетику, ритейл, транспорт и логистику, а также медицинских и фармацевтических компаний.

Как отметили представители свыше 40% компаний, доступ к информационным ресурсам организаций под учетными записями сотрудников сохраняется и после их увольнения. Самой частой причиной такого развития ситуации становится несогласованность действий кадровых служб и ИТ-подразделений, ответственных за управление доступом к цифровым активам организаций. Как показывает практика, такие учетные записи могут существовать в корпоративных информационных системах продолжительное время, а уволенные сотрудники сохраняют доступ к цифровым активам своего бывшего работодателя.

Если в компании не внедрены процедуры регулярного обновления парольной политики, именно эти учетные записи чаще всего и становятся точкой входа для киберпреступников. Опыт нашей компании показывает, что в настоящее время предприятия и организации в первую очередь заинтересованы в решениях, обеспечивающих управление доступом и защиту данных.

## Что делать?

Сегмент информационной безопасности активно развивается. Одна из доминирующих на нем тенденций заключается в том, что технологии ИИ все активнее проникают в традиционные средства защиты информации. Так, DLP-системы используются для предотвращения утечек информации, детектирования чувствительных данных, выявления аномалий в поведении пользователей и устройств. Например, ИИ-модуль, интегрированный в системы отечественных вендоров, детектирует графические файлы, содержащие конфиденциальную информацию, – изображения банковских карт, сканы паспортов, другую не менее важную коммерческую документацию.

Как отметили представители свыше 40% компаний, доступ к информационным ресурсам организаций под учетными записями сотрудников сохраняется и после их увольнения.

Благодаря реализации такого подхода, удается повысить скорость реагирования сотрудников, отвечающих на информационную безопасность, на опасные инциденты. Встроенная в систему нейросеть распознает речь на 50 языках и переводит ее в текст. Все эти данные тоже используются для расследования утечек информации и действий инсайдеров в компаниях.

В свою очередь, IdM-системы, которые также широко представлены на российском рынке, позволяют предупредить или снизить ущерб от утечек информации при комплексном подходе к решению задач в сфере кибербезопасности. Например, при интеграции с системами контроля и управления доступом они повышают безопасность информационных систем и исключают возможность использования чужих учетных записей.

В интеграции с продуктами класса SIEM (Security information and event management), управляющими событиями безопасности, IdM-система отправляет данные в SIEM для анализа, предотвращения и расследования инцидентов в области информационной безопасности.

Применение технологии SSO (Single Sign-On) и мультифакторной аутентификации наряду с IdM-решением позволяет выстроить безопасный вход в различные сервисы именно благодаря использованию единого набора учетных данных. Совместная работа платформ IdM и PAM (Privileged Access Management) обеспечивает управление доступом привилегированных пользователей к конфиденциальной информации, критичным бизнес-процессам и информационным системам.

Рассмотренные механизмы противодействия злоумышленникам остаются весьма актуальными для предприятий, организаций и компаний из различных сегментов экономики, поскольку, по прогнозам экспертов, в 2025 г. увеличится число инцидентов, связанных с кражей конфиденциальных корпоративных данных, перехватом ключевых сервисов, уничтожением инфраструктуры, взломом информационных ресурсов подрядчиков для доступа к целевым сетям. Поэтому специалисты в сфере информационной безопасности рекомендуют включить решения класса DLP, IDM- и PAM-системы, а также DAG/DCAP-платформы в контур инфраструктуры для защиты данных и противодействия утечкам. ■