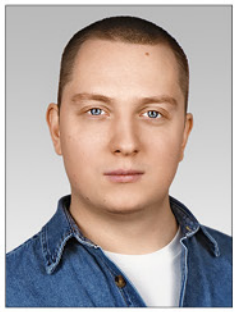

Иван РОГАЛЕВ
руководитель отдела разработки платформенных решений BI.ZONE

Антон СВИНЦИЦКИЙ
директор по консалтингу АО «ДиалогНаука»

БЕЗОПАСНОСТЬ СВЕРХУ ВНИЗ

КАК ПОСТРОИТЬ ИБ-ЭКОСИСТЕМУ ДЛЯ ДОЧЕРНИХ ОБЩЕСТВ

Крупная компания защищена настолько, насколько защищены её дочерние организации — такой вывод можно сделать и по итогам атак в 2022 году, и по более ранним инцидентам. Поговорим о том, как изменить подходы к безопасности, чтобы статистика таких случаев стремилась вниз.

Владельцы экосистем и крупных холдингов прежде всего думают о безопасности головной компании. При этом взлом дочерней организации даёт злоумышленникам множество возможностей, чтобы развить атаку. Так что последствия такого взлома затронут и другие организации экосистемы или холдинга.

Например, в октябре 2022 года взломанный почтовый сервер некой организации открыл хакерам доступ к серверам Организации по атомной энергии Ирана. Скомпрометированными оказались закрытые данные о работе Бушерской АЭС, паспорта и визы иранских и российских специалистов со станции, контракты по ядерным разработкам и др.

Крупным бизнес-структурам сейчас не хватает понятных и удобных решений, которые позволили бы контролировать информационную безопасность (ИБ) во всей группе компаний. Эту проблему рынку предстоит решить в 2023 году.

ЗАЧЕМ ОБНОВЛЯТЬ ПОДХОДЫ

Большинство сегодняшних ИБ-решений направлены на защиту одной конкретной организации. В результате при взгляде на крупную экосистему картина выходит хаотичная.

1. Отсутствует стандартизация и контроль безопасности всех дочерних организаций

- Разрозненные коммуникации
- Отсутствие регулярного контроля
- Нет оперативной информации о текущем уровне защищённости дочерних обществ и о свойственных им угрозах

2. Нет отлаженной работы между организациями группы

- Каждый CISO решает задачу по-своему
- Не прописаны сценарии действий, в том числе при выходе инцидентов за пределы одной организации

3. Средства защиты в дочерних обществах внедряются хаотично

- Инструменты не связаны между собой
- Ряд инструментов работает не в полную силу
- Некорректно настроены правила
- Разрозненные и мультивендорные решения увеличивают стоимость владения и поддержки

4. Нет баланса знаний в каждой организации

- Большое количество компетенций в головной организации и малое в дочерней
- Нет опыта управления системами безопасности в дочерних обществах

В крупной инфраструктуре все компоненты взаимно интегрированы, идёт постоянное обогащение информации, чтобы компания получила больше прибыли. Такая экосистемная архитектура требует новых подходов к кибербезопасности.

Каждая дочерняя организация вносит вклад в общую защиту от современных киберугроз. А использование единой платформы позволяет систематизировать и автоматизировать работу над повышением уровня кибербезопасности, принимать взвешенные управленческие решения, управлять задачами и отслеживать результаты такой деятельности.

КАК ЭТО МОЖЕТ ВЫГЛЯДЕТЬ

Платформа для централизованного управления масштабными ИТ-структурами поможет решить две проблемы. Во-первых, это интеграция сервисов безопасности во всём холдинге. Во-вторых, с возникающими проблемами можно бороться, ориентируясь сразу на всю группу компаний и выстраивая взаимодействие между дочерними обществами.

Добиться этих целей позволит набор функций, который реализован, например, в решении BI.ZONE Cyber Maturity Platform (CMP). Компания BI.ZONE развивает его в партнёрстве с интегратором «ДиалогНаука» (рис. 1).

Какие возможности нужны для управления кибербезопасностью в холдинге:

- инвентаризация ИТ-активов;
- информирование об угрозах и опросы сотрудников по итогам инцидентов;
- стандартизация требований с учётом особенностей каждой компании, входящей в экосистему (холдинг);
- аудит соответствия требованиям (с возможностью сравнения результатов организации как в определённом промежутке времени, так и с другими участниками экосистемы);
- планирование деятельности и контроль выполнения планов и мероприятий;

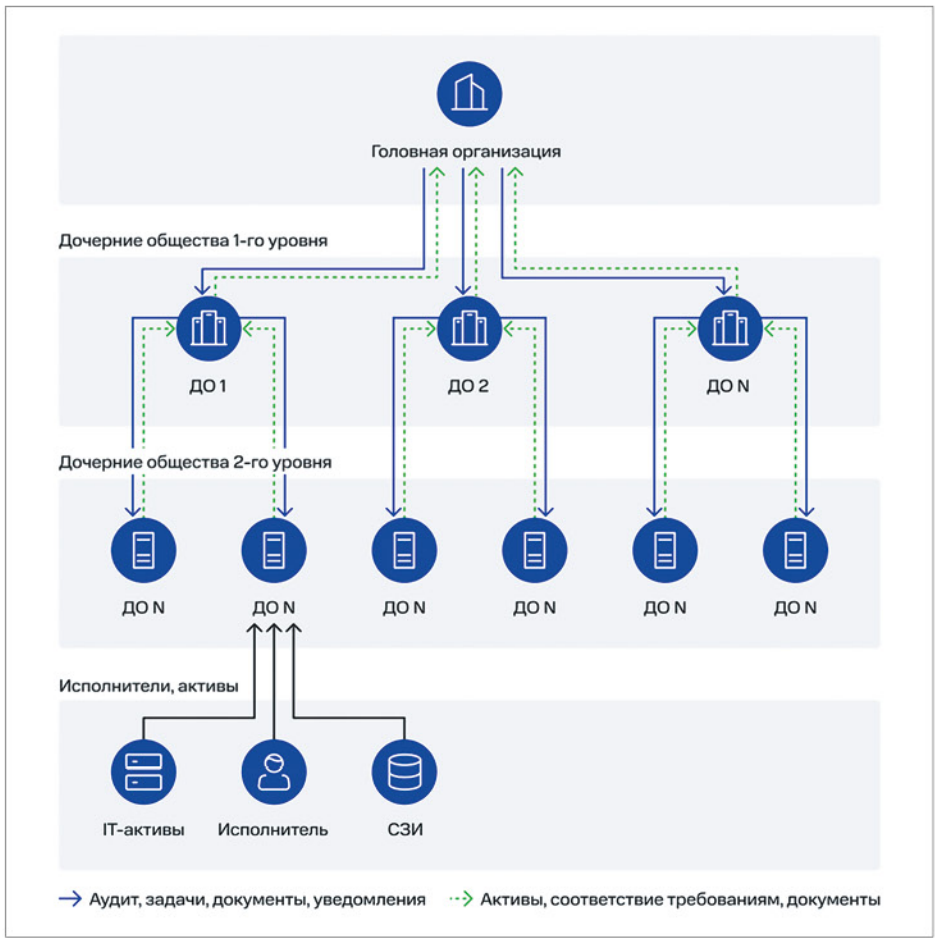

Рисунок 1. Управление информационной безопасностью в холдинге

- внедрение нормативных документов;
- управление инцидентами;
- управление знаниями;
- формирование отчётности и аналитика.

Выгоду от такого «зонтика» кибербезопасности получают все участники.

ЦЕННОСТЬ ДЛЯ ГОЛОВНОЙ ОРГАНИЗАЦИИ

Ключевое преимущество — централизованный контроль кибербезопасности во всей группе компаний. Инвентаризация активов кибербезопасности, отслеживание исполнения планов по ИБ, повышение осведомлённости сотрудников об угрозах.

Помимо этого, головной компании становится проще масштабировать опыт и технологии на всю экосистему. Инструменты аналитики позволяют специалистам выгружать отчёты по необходимым срезам данных. Автоматизация рутины по инвентаризации средств защиты разгружает сотрудников кибербезопасности и сокращает ИТ-трудозатраты. Руководство группы компаний получает актуальную информацию о том, какие системы используют дочерние общества и могут получить у поставщиков скидки, учитывая общий объём используемого ПО. Помимо экономии на таких соглашениях, компания сокращает затраты на обслуживание средств защиты: на месте «зоопарка» систем появляется упорядоченная архитектура.

ЦЕННОСТЬ ДЛЯ ДОЧЕРНЕЙ ОРГАНИЗАЦИИ

Дочерние компании, в свою очередь, могут выстроить удобное операционное управление уровнем осведомлённости сотрудников и активами кибербезопасности. Совместное использование знаний на уровне группы компаний помогает соответствовать требованиям головной организации и регуляторов. В результате во всей структуре быстро формируются зрелые процессы.

Только за последний год компании столкнулись с волной эксплоитов, которые грозили серьёзными последствиями для компаний. Уязвимости в Apache Log4j, Fortinet, Microsoft Exchange — можно вспомнить ещё много примеров. Единая платформа, охватывающая весь ландшафт группы, помогает реагировать на такие угрозы за дни или часы.

Методология BI.ZONE CMP позволяет оценивать уровень зрелости кибербезопасности в дочерних обществах и определять их вектор развития. Она включает почти 30 направлений: от архитектуры и стратегии до управления уязвимостями и тестов на проникновение.

Выбор из 900 метрик позволяет оценить по единому подходу разрозненный бизнес из множества организаций. Результаты анализа покажут, где каждый участник находится на шкале защищённости и в каком направлении ему следует развиваться с точки зрения безопасности.

Этапы применения методологии:

1. Планирование
   - сбор информации, инвентаризация ИТ-активов;
   - определение целевого уровня, профилирование организации.
2. Реализация
   - подготовка требований по ИБ;
   - создание шаблонных документов и приказов;
   - стандартизация конфигураций;
   - настройка внешних технических сервисов ИБ;
   - внедрение типовых решений подсистем защиты.
3. Контроль
   - стандартизация обеспечения ИБ в дочерних организациях;
   - определение текущего уровня ИБ;
4. Совершенствование
   - рекомендации по устранению несоответствий;
   - планы реализации мероприятий.

2023 ГОД — ГОД ПРОАКТИВНОСТИ

Угрозы нужно устранять превентивно, а для этого компаниям следует помнить: безопасность начинается на периметре самого отдалённого дочернего общества. Если её инфраструктура защищена так же, как в головной организации, вероятность пострадать от кибератаки сильно снижается.