Особенности защиты информации на промышленных предприятиях

Подходы к выстраиванию комплексной системы информационной безопасности критически важных производственных предприятий, нуждающихся в обеспечении целостности, доступности и конфиденциальности информации, имеют свои особенности и специфику, которые должны быть учтены еще на этапе построения концепции защиты. Попробуем рассмотреть основные моменты снижения рисков и борьбы с угрозами в инфраструктуре промышленных предприятий.

Информационная безопасность холдинга

Как в промышленности, где чаще всего мы имеем дело с сетью распределенных предприятий, объединенных "под крылом" одной или нескольких управляющих компаний, так и в других территориально распределенных организациях в настоящее время активно идет процесс централизации подходов к управлению ИТ-инфраструктурой, внедряются централизованные системы управления предприятием, централизуются ИТ-ресурсы. Это автоматически влечет за собой необходимость выстраивания централизованной организационной схемы управления информационной безопасностью и внедрения централизованных средств защиты информации. В связи с этим отдельные филиалы, которые раньше работали с определенной долей независимости, в том числе и самостоятельно управляли информационной безопасностью на своих предприятиях, начинают подчиняться центральной службе ИБ, расположенной в головном предприятии.

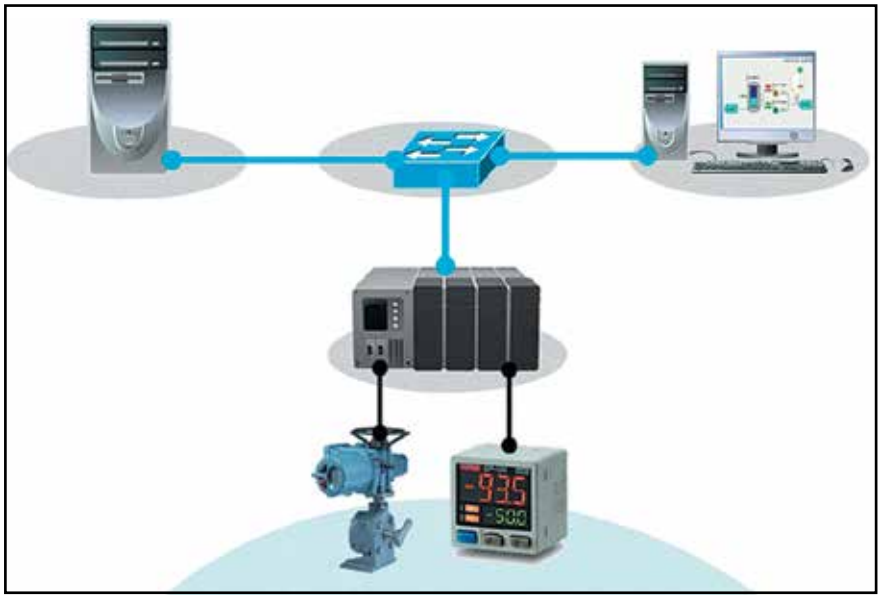
Соответственно, на уровне головного предприятия сосредотачиваются функции формирования и контроля исполнения единых (отраслевых) требований к защите, а филиалам отводятся функции исполнения требований и предоставления отчетности. Причем нередко исполнительскую функцию отдают на аутсорсинг внешним или внутренним сервисным организациям с собственной филиальной сетью внутри холдинга.

С технической точки зрения происходит похожий процесс: если раньше на отдельных предприятиях был свой подход к построению архитектуры ИБ, выбору вендоров и внедрению решений, то с централизацией происходит переход на единую "шкалу измерения". Происходит унификация и стандартизация средств защиты информации, направленная на реализацию централизованных механизмов защиты и контроля.

Информационная безопасность технологических процессов

Среди угроз, которые несут опасность для технологических процессов, находятся как природные катаклизмы и аварии, так и действия организованных террористических группировок и хакеров, которые могут быть предприняты с целью коммерческой наживы либо в рамках политической/информационной войны. Например, уже известны случаи хакерских атак на энергетические компании США, металлургический завод в Германии, украинских поставщиков электроэнергии и пр. Поэтому, когда на кону стоит либо потенциальный вывод из строя доменной печи, либо сбой в региональном энергообеспечении, необходимо обеспечить адекватный баланс между безопасностью и автоматизацией.

Автоматизированные системы управления технологическими процессами работают на базе специфических сетевых стандартов, требующих специализированных инструментов анализа и мониторинга активности. Такие системы нередко достаточно статичны, базируются на устаревшем программном обеспечении и могут крайне болезненно реагировать на любые изменения, в том числе и те, которые потенциально могли бы повы-



Упрощенная схема взаимосвязей в рамках функционирования промышленной системы

сить уровень безопасности. В некоторых случаях такие мероприятия могут негативно повлиять на производительность АСУ ТП либо иным образом нарушить функционирование ее компонентов.

Поэтому к основному типу инструментов, которые здесь могут быть успешно использованы, относятся пассивные системы мониторинга активности и предотвращения угроз (Network Anomaly Detection), которые встраиваются в существующую инфраструктуру (например, подключаются к SPAN-порту) и пассивно прослушивают весь циркулирующий трафик, обнаруживая аномальные отклонения и уведомляя службы безопасности о необходимости расследование того или иного инцидента.

Рассмотрим, например, системы мониторинга сетевых аномалий (NBAD, Network Behavior Anomaly Detection), осуществляющие анализ сетевого трафика на предмет выявления признаков атак. Применение подобного класса решений может помочь обнаружить активность вредоносного софта, аналогичного Stuxnet или BlackEnergy. Правда, для обнаружения аномального содержимого прикладных промышленных протоколов понадобится более расширенный функционал решений класса Deep Packet Inspection или Industrial Network Anomaly Detection (INAD).

Стоит отметить, что в какой-то степени АСУ ТП даже несколько проще с точки зрения пассивного анализа сетевого трафика по сравнению с корпоративными системами, поскольку картина информационных потоков в АСУ ТП довольно статична. А значит, даже мельчайшие отклонения в трафике можно обнаружить легче в отличие от аналогичных систем обнаружения аномалий в корпоративных сетях, где характеристики меняются весьма динамично, а связи между различными хостами сильно переплетены.

Ко второму типу решений для обеспечения безопасности АСУ ТП относятся так называемые активные инструменты управления информационными потоками и доступом. Речь идет об обычных и промышленных межсетевых экранах, решениях для защиты конечных узлов и управления доступом к сети, однонаправленных шлюзах и т.п.

При этом всегда нужно помнить, что на начальном этапе построения защиты АСУ ТП необходимо сформировать отраслевые требования, поскольку промышленные системы специфичны, и требования к обеспечению их безопасности должны учитывать эту специфику. Для атомной промышленности они – одни, для сталелитейного завода – другие, для двигателестроения – третьи. Поэтому значимость угроз и потенциальный негативный ущерб в случае успешной атаки на соответствующую систему могут существенно различаться.

Обеспечение комплексной безопасности промышленной инфраструктуры

Обеспечение комплексной безопасности инфраструктуры промышленного предприятия имеет свою специфику. Например, если мы имеем дело с десятками промышленных цехов, распределенных на территории в несколько десятков квадратных километров, то для доступа к корпоративным ресурсам могут потребоваться беспроводные точки подключения (Wi-Fi), которые также нужно контролировать. Если разнородные централизованные информационные системы концентрируются в едином дата-центре, через который идут все потоки информации, то может потребоваться реализация единой системы управления учетными данными пользователей (системы класса IDM).

Если же речь идет об обеспечении безопасного мобильного доступа к информационным ресурсам предприятия, то для этого могут быть использованы распространенные сейчас MDM-системы, позволяющие управлять мобильными устройствами. Например, несколько лет назад специалисты компании КРОК помогли ОАО "Авиадвигатель", где работают более 2 500 человек, обеспечить для сотрудников доступ к основным корпоративным приложениям с их собственных мобильных устройств. В рамках проекта было внедрено комплексное решение, состоящее из MDM-системы и подсистемы SSL VPN для защищенного доступа к внутренним ИТ-ресурсам предприятия.

Но в целом, если вынести за скобки методы защиты АСУ ТП и отраслевую специфику, то комплексный подход к защите информации на промышленном предприятии будет примерно тем же, что и на любом другом территориально распределенном предприятии. В отличие от банков или сотовых операторов, где отраслевые требования к информационной безопасности задаются внешним регулятором, в промышленности их определяет собственник холдинга или совет директоров, который может определить ту или иную парадигму защиты, четко учитывающую основные риски и угрозы.

Исключением является только вопрос защиты АСУ ТП, поскольку в скором будущем может появиться соответствующий федеральный закон. Кроме того, ряд важных вопросов затрагивает и обновленная доктрина информационной безопасности, в которой рассматриваются в том числе и возможности воздействия на предприятия оборонно-промышленного комплекса, а также подписанный в конце прошлого года Указ Президента Российской Федерации N 683 "О Стратегии национальной безопасности Российской Федерации". Кроме того, существует документ Совета Безопасности РФ, определяющий "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации". И, наконец, – приказ ФСТЭК России №31, определяющий требования к обеспечению защиты информации в АСУ ТП.

С другой стороны, если промышленное предприятие стремится в будущем осуществлять экспорт продукции на зарубежные рынки или выйти на IPO, то для этого может оказаться полезным подтвердить соответствие выстроенной системы управления информационной безопасностью (СУИБ) требованиям международного стандарта ISO/IEC 27001:2013 (или 2005). В частности, на приведение собственной СУИБ компании КРОК в соответствие с требованиями ISO/IEC 27001:2013 ушло

всего порядка полугода, и специалисты компании активно используют имеющийся опыт во внешних проектах.

И наконец, не стоит забывать про общие для всех отраслей требования 152-ФЗ по защите персональных данных. Постановление Правительства №1119 от ноября 2012 года обязывает организации проводить проверку соответствия систем защиты персональных данных не реже, чем раз в три года. Это можно осуществлять как самостоятельно, так и с помощью привлеченных консультантов при наличии у них соответствующей лицензии, выданной ФСТЭК России.

Что касается соблюдения положений №242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях", согласно которому базы с персональными данными российских граждан должны находиться на территории России, то чаще всего на отечественных предприятиях его требования обеспечиваются изначально. Однако для учета всех требований закона помощь внешних консультантов в рамках аудита ИТ-инфраструктуры и процессов может быть полезна зарубежным компаниям с российскими представительствами.

И еще немного об особенностях промышленной инфраструктуры

Многие технологии, применяемые в промышленности, изначально были изолированы друг от друга, поэтому угрозы информационной безопасности были для них не столь актуальны. Однако постепенно происходит как объединение классических офисных систем с АСУ ТП, так и переход на единые унифицированные стандарты. Например, в наши дни распространенное явление – переход промышленности на обычные для корпоративных систем протоколы связи, в то время как раньше использовались только промышленные.

В целом, средства защиты АСУ ТП с точки зрения отраслевой специфики можно условно разделить на классические (применяемые для защиты корпоративных систем) и специализированные, которые подходят для использования в условиях агрессивной окружающей среды (высокие температуры, магнитные излучения, пыль, влага и пр.). Условия среды должны быть в обязательном порядке учтены в процессе проработки концепции информационной безопасности с целью минимизации их негативного влияния. На практике это означает использование устойчивого к агрессивным средам промышленного оборудования (специальные корпусы, отказоустойчивые вентиляторы и пр.) и его специального монтажа. Этот, казалось бы, не самый главный нюанс с позиции безопасности может существенным образом снизить риск остановки производства и возникновения аварийной ситуации.

Андрей Заикин, руководитель направления информационной безопасности,
Евгений Дружинин, ведущий эксперт направления информационной безопасности,
компания КРОК

07–09 июня 2016 года в Москве в гостиничном комплексе «Измайлово» (четыре звезды) состоится старейшая в нашей стране, уже XIX по счету, ежегодная международная научно-ПРАКТИЧЕСКАЯ конференция

ИБММ

07 – 09 июня 2016 года

«ИТ–БИЗНЕС в МЕТАЛЛУРГИИ, МАШИНОСТРОЕНИИ, ТЭК, ХИМИИ и РИТЕЙЛЕ»

Организатор: компания «ИБММ.РУ»(*www.ibmm.ru*)






В ходе проведения конференции 2015 года (вопреки кризису) были получены следующие **результаты**:

1. в ней приняло участие 193 юридических лица. Среди них **173 предприятия**: оборонного комплекса (ОПК), гражданского машиностроения, металлургии, горнорудного и горнодобывающего комплексов (ГДК), энергетики, а также нефтегазовой, нефтеперерабатывающей, нефтехимической, химической и фармакологической промышленности и 20 IT - компаний;;
2. **90 %** отраслевых предприятий были представлены IT-директорами и/или TOP-менеджерами;
3. в программу конференции оргкомитетом было отобрано **36 докладов**, причем 70% из них (**25**) составили доклады промышленных предприятийй;
4. в 2015 году в нашем форуме приняли участие 305 делегатов;
5. мы получили от участвовавших в ИБММ–2015 промышленных предприятий и IT-компаний **79 отзывов** и они продолжают поступать к нам практически ежедневно.

С программой, подробным фотоотчетом, а также слайд-шоу и аудиозаписями всех 36 докладов ИБММ–2015 можно познакомиться на www.ibmm.ru/ОтчетИБММ.

Миссия ИБММ: Среди целого ряда периодических конференций и форумов по проблемам информационно-коммуникационных технологий (ИКТ) конференция «ИБММ» занимает заметное место, отличаясь от других мероприятий:

- Концентрацией внимания на практике внедрения, эксплуатации и сопровождения ИТ-решений. Конкретно: на опыте решения прикладных задач уровня предприятия с охватом большинства стадий жизненного цикла разработки и производства разнообразной наукоемкой продукции в наиболее «продвинутых» отраслях промышленности и ритейле.
- Внимательным отношением к особенностям адаптации существующих инструментов и международного опыта управления предприятиями и ритейл-компаниями с учетом отраслевой специфики для предприятий и ритейл-компаний разного масштаба и различного характера производства.
- Обсуждением оригинальных отечественных разработок программно-аппаратных средств и опыта импортозамещения.
- Вниманием к интеграции различных прикладных задач и др.

Помимо этого, наша конференция объединяет усилия специалистов по коллективному созданию библиотеки передового отечественного и международного опыта информатизации бизнес процессов. И каждый участник может им творчески воспользоваться для своего предприятия или ритейл-компании, сократив сроки разработки и уменьшив стоимость работ по своему проекту. Тем более, что организаторы конференции обеспечивают для этого максимально комфортные условия.

До скорой встречи на ИБММ–2016 !

Генеральный директор «ИБММ.РУ»,
Директор конференции, к.х.н. - Дмитрий Виницкий
+7 (495) 544-19-57, +7 (916) 752-08-52 dmv@ibmm.ru

www.ibmm.ru