Кибербезопасность промышленных систем. Практикум по программе «Лаборатории Касперского». Обучить самое уязвимое

Защита непрерывности производства и повышение осведомленности персонала в области кибербезопасности – актуальная задача на любом предприятии, а тем более на промышленном производстве, где технологический процесс ведется под управлением автоматизированных систем. Международная образовательная компания ООО «Абирой» проводит курсы по кибербезопасности промышленных систем, повышающие осведомленность руководящего состава, рядовых сотрудников предприятий, а также специалистов в области безопасности IT/OT. Вместе со статьей опубликовано интервью с сотрудником департамента программ обучения кибербезопасности ООО «Абирой» Л.А. Ризвановым.

ООО «Абирой», г. Иннополис, Республика Татарстан

Осведомленность о киберугрозах в промышленной среде

Неэффективная система кибербезопасности (или ее отсутствие) может слишком дорого обойтись промышленному предприятию. По статистике The Business Advantage Group[1], опубликованной в начале 2017 года, 54% промышленных предприятий в 2016 году пережили от одного до пяти происшествий в сфере информационной безопасности. И это несмотря на то, что нужность и важность кибербезопасности уже никем не оспариваются, а в промышленных структурах тем более. Но, как ни парадоксально, до сих пор защита от киберугроз срабатывает далеко не всегда, причем главным образом из-за незнания и неподготовленности сотрудников компаний к столкновению с ними. Более чем в 80% случаев нарушение правил информационной безопасности вызвано человеческим фактором. А учитывая, что кибератаки в основном используют именно человеческий фактор и при этом непрерывно эволюционируют, одна из лучших мер защиты – повышение культуры кибербезопасности сотрудников.

В мире ведутся разработки, призванные решить эту актуальную задачу. В основном ими занимаются хорошо известные компании с популярным брендом и многолетней историей. Так, «Лаборатория Касперского», один из лидеров в области информационной безопасности, создает программы для обучения персонала, помогающие сотрудникам промышленных предприятий приобрести эффективные навыки по обеспечению кибербезопасности и препятствию киберинцидентам. Обучающие программы входят в портфолио Kaspersky Industrial CyberSecurity – набор технологий и сервисов для защиты ключевых уровней промышленных систем, включая серверы SCADA, операторские панели, инженерные рабочие станции, ПЛК и сетевые соединения. Решение создано для специалистов, непосредственно работающих

▲ Постер «Лаборатории Касперского» с правилами кибербезопасности

[1] Английская компания, занимающаяся исследованиями бизнеса, маркетинга и управленческого консалтинга на рынке IT-технологий и телекоммуникаций.

с АСУ ТП и производственным оборудованием, а также для специалистов в области безопасности IT/OT.

В стремлении повысить осведомленность рынка о проблемах промышленной кибербезопасности «Лаборатория Касперского» вовлекает в проведение обучающих программ не только собственных экспертов, но и партнеров. Сотрудничество с «Абирой» – успешный пример продвижения партнером экспертизы «Лаборатории Касперского» среди конечных заказчиков.

Богатый опыт в формировании культуры кибербезопасности на промышленных предприятиях накоплен компанией «Абирой» (Abiroy). Одну из основных специализаций этой международной образовательной компании можно кратко обозначить как «безопасность на рабочем месте». Здесь помогают создать или усовершенствовать навыки безопасного поведения сотрудникам предприятий электроэнергетики, нефтехимической и нефтегазовой отраслей, металлургии, машиностроения, а также международных компаний. «Абирой» – аккредитованный тренинговый центр для проведения программ таких профессиональных организаций, как Международная академия нефти и газа OPITO, Национальный экзаменационный совет Великобритании по охране труда (NEBOSH) и Институт по технике безопасности и охране труда на производстве (IOSH). В 2005–2017 годах обучение под руководством специалистов «Абирой» прошли свыше 5000 сотрудников нефтегазовых и энергетических компаний России, Казахстана, Азербайджана и Узбекистана. Среди клиентов «Абирой» – ПАО «ЛУКОЙЛ», ОАО «ЯМАЛ СПГ», ПАО «Интер РАО», ПАО «ГМК «Норильский никель», «ПетроКазахстан», Karachaganak Petroleum Operating B.V. и др.

С 2017 года компания «Абирой» провела обучение сотрудников нескольких десятков предприятий. Одним из масштабных проектов было обучение персонала «АВТОВАЗа». Очные тренинги были проведены для 170 сотрудников компании. Участники получили актуальные знания о киберугрозах для промышленных предприятий, методах защиты и реагирования на инциденты, а также узнали, как выполнять анализ вредоносного ПО и простое цифровое расследование. Важное направление в работе компании «Абирой» – обучение правилам кибербезопасности, которые приобретают особую актуальность в этом году, после того как 1 января 2018 года вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

Поскольку понятие «кибербезопасность промышленных систем» для сотрудников, занимающих разные должности, может подразумевать разные меры, обучающие курсы, которые проводит компания «Абирой», сегментированы для специалистов, руководителей отделов ИТ, ИБ, АСУ, СБ, диспетчеризации и сотрудников других подразделений, использующих АСУ ТП. Кроме повышения культуры кибербезопасности компания «Абирой» дает специальные рекомендации по внедрению лучших практик и средств безопасности.

Особенности курсов по кибербезопасности промышленных систем, или Как повысить культуру кибербезопасности

Сегодня организации тратят миллионы, чтобы повысить культуру кибербезопасности сотрудников, однако руководители департаментов информационной безопасности редко остаются довольны результатами. Почему так происходит? Большинство тренингов по кибербезопасности промышленных систем носят общий характер, затянуты, изобилуют техническими подробностями или фокусируются на негативных аспектах. Эти программы не учитывают способности людей самостоятельно принимать решения и учиться, а в результате оказываются неэффективными. К тому же они не отражают реальных угроз, с которыми сталкиваются сотрудники промышленных предприятий.

Курсы, разработанные «Лабораторией Касперского», которые «Абирой» проводит с применением образовательных методик и элементов интерактивного обучения, более эффективны, поскольку направлены на изменение поведения. Они поощряют стремление каждого сотрудника к безопасной, ответственной работе. В результате создается корпоративная среда, в которой соблюдение правил кибербезопасности является естественной частью работы.

Обучение охватывает широкий ряд проблем безопасности: от базовых правил до атак с использованием вредоносного ПО. Поднимаются вопросы утечки данных и безопасного использования социальных сетей. Для обучения применяется набор простых упражнений.

Обучающие курсы по кибербезопасности промышленных систем охватывают широкий круг тем.

- Обзор существующего ландшафта угроз, проблем безопасности, проявлений человеческого фактора, сетевых атак на АСУ ТП.
- Сетевая безопасность IT-систем и АСУ ТП: особые соображения.
- Практический пример, демонстрирующий использование методов предотвращения, обнаружения и устранения угроз.
- Соответствие промышленным стандартам и правовым нормам.
- Топологии сетей и принципы работы технологий сетевой безопасности.
- Роли и структура рабочих групп по кибербезопасности.
- Распространенные ошибки в области кибербезопасности.
- Понимание существующего ландшафта киберугроз для промышленных сред и методов борьбы с атаками, направленными на вашу отрасль или организацию.
- Идентификация и выявление инцидентов информационной безопасности.
- Проведение неэкспертных расследований.
- Составление и осуществление эффективного плана реагирования на инциденты.

Курсы проводятся в двух форматах:

- открытом (занятия для сотрудников различных предприятий региона);
- корпоративном (мероприятия на территории заказчика, курс адаптируется к его отрасли).

Участники овладевают навыками культуры кибербезопасности и приобретают знания в сотрудничестве с экспертами мирового класса, которые делятся собственным опытом

прогнозирования, предотвращения, обнаружения и устранения киберугроз. Курсы включают как теоретические, так и практические, лабораторные, занятия. По завершении каждого курса участникам выдаются сертификаты от «Абирой» и «Лаборатории Касперского», удостоверение о повышении квалификации установленного образца.

ООО «Абирой», г. Иннополис,
Республика Татарстан,
тел.: +7 (800) 333-4938,
e-mail: info@abiroy.com,
сайт: cyber.abiroy.com

Вместо послесловия.

Интервью с Линаром Альбертовичем Ризвановым, сотрудником департамента программ обучения кибербезопасности ООО «Абирой»

ИСУП: Как давно вы начали сотрудничать с «Лабораторией Касперского» и насколько его программы по кибербезопасности пользуются спросом?

Л. А. Ризванов: Сотрудничество с «Лабораторией Касперского» началось в 2017 году. Программы по кибербезопасности пользуются нарастающим спросом. Есть несколько предпосылок:

- нарастающие киберугрозы в промышленном секторе (АСУ ТП, SCADA). Промышленное оборудование слабо защищено, так как большинство оборудования устарело и не проектировалось с учетом информационной безопасности. Киберпреступники находят уязвимости и занимаются целевыми атаками на промышленный сектор в целях нанесения физического ущерба предприятиям, регионам и государству в целом;
- законодательная база. С 1 января 2018 года вступил в силу и обязателен к исполнению 187-ФЗ РФ «О безопасности критической информационной инфраструктуры Российской Федерации». В законе формулируются требования по осуществлению мер защиты критически важных объектов РФ, неисполнение которых влечет и уголовную ответственность. В рамках закона имеется комплекс мер по защите, в который входит обучение и повышение осведомленности персонала в области кибербезопасности.

ИСУП: На каком этапе ваших курсов по кибербезопасности промышленных систем слушатели начинают воспринимать это не как обязаловку, а как информацию, полезную для себя?

Л. А. Ризванов: Все участники курсов понимают важность кибербезопасности. Наш практикум расширяет эту тему и на практических занятиях показывает, насколько легко злоумышленники могут проникнуть в изолированную сеть и управлять технологическими процессами. На этапе практики участники осознают, насколько тема «подкралась близко» и что ее игнорирование может обернуться реальной кибератакой. Ведь необязательно быть объектом атаки, чтобы стать ее жертвой.

ИСУП: В чем ключевая разница между занятиями для руководителей, инженерного состава и рядовых сотрудников?

Л. А. Ризванов: Программы адаптированы к потребностям аудитории. Курсы для руководителей направлены на обеспечение бесперебойной работы предприятия. В результате обучения топ-менеджмент приобретает понимание ответственности перед бизнесом и надзорными органами, меняет свое представление о страховых рисках, перенимает методики уменьшения вероятности сбоев в работе производства вследствие кибератак. На курсе даются рекомендации по организационной структуре. Программа учитывает занятость руководящего состава и длится полдня.
Программа для рядовых сотрудников основана на осознанном следовании политике информационной безопасности. Сотрудники обучаются противодействию методам социальной инженерии, идентификации киберугроз и реагированию на киберинциденты. Программа длится полдня.
Практикум для специалистов и инженерного состава длится два дня и наиболее полно охватывает вопросы кибербезопасности АСУ ТП и SCADA. Практикум нацелен на повышение осведомленности специалистов и практическую отработку полученных знаний. По итогам обучения проводится экзамен, выдаются официальные сертификаты от «Лаборатории Касперского» и «Абирой», документ о повышении квалификации установленного государственного образца.

ИСУП: Как проходят тренинги? Можете ли вы описать одну из реальных ситуаций с нарушением правил кибербезопасности, которую вы используете в своих тренингах?

Л. А. Ризванов: В рамках практикума рассматриваются кибератаки на различные промышленные предприятия, разбираются уязвимости, используемые злоумышленниками, и векторы кибератак. География рассматриваемых киберинцидентов охватывает весь мир. Информация о рассматриваемых реальных кейсах доступна только участникам практикума и полностью конфиденциальна. Все участники практикума подписывают соглашение о неиспользовании полученных знаний в неправомерных целях.

Беседовал С. В. Бодрышев,
главный редактор журнала «ИСУП»