Реальность в защите КИИ. Практические кейсы от бизнеса

Антон Шипулин
CISSP, CEH, CSSA
Менеджер по развитию решений
по безопасности критической инфраструктуры
Лаборатория Касперского

KASPERSKY

КВАЛИФИКАЦИЯ СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ И АСУ ТП

AGC

- AGC Glass Germany GmbH с 2003 года поставляет автомобильное стекло таким ведущим производителям, как BMW, Volkswagen, Mercedes-Benz, Volvo и Opel. На предприятии компании в Вегберге (рядом с Мёнхенгладбахом, Германия) работают 150 человек. AGC входит в состав Asahi Glass Company – японской группы, являющейся крупнейшим в мире производителем стекла, обеспечивающим 50 000 рабочих мест в 20 странах мира.

- AGC Glass Germany GmbH обрабатывает стекло для автомобилей, изготовленное на других предприятиях группы, в соответствии с конкретными потребностями клиентов: например, устанавливает на стекло системы обогрева, датчики дождя или уплотнители. После этого компонент поступает на производство различных автомобилестроителей.

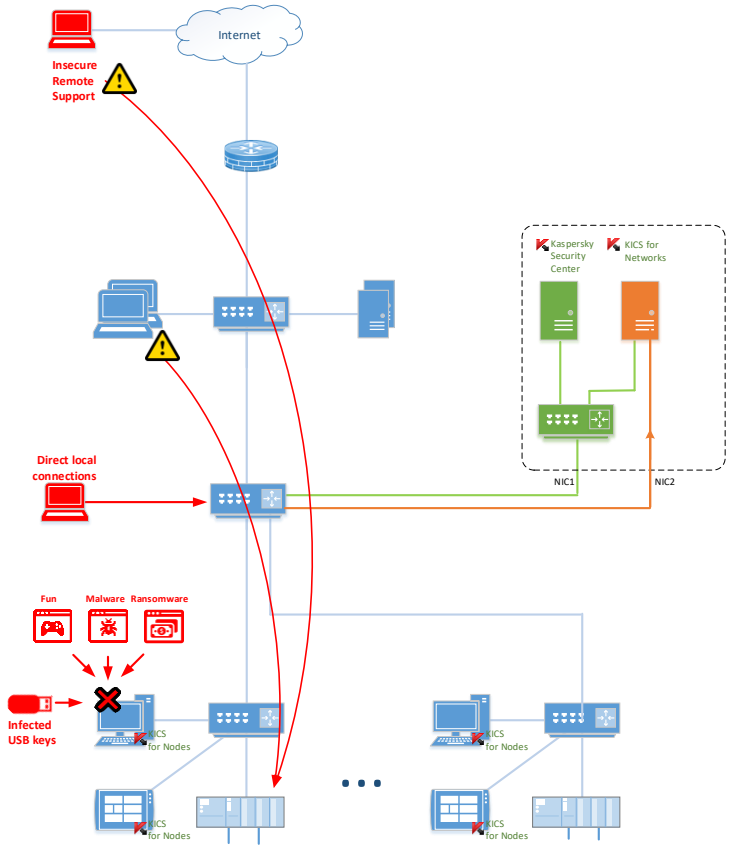
Завод

- AGC производит стекла для автомобильных компаний. Завод имеет 12 производственных линий. Использует промышленные контроллеры известного мирового производителя для управления технологическим процессом

- Каждая производственная линия имеет один контроллер и HMI или станцию оператора. Данные между HMI и ПЛК передаются по промышленному протоколу производителя

Завод

- Каждая отдельная производственная линия на предприятии AGC защищена решением Kaspersky Industrial CyberSecurity. Решение отслеживает события на всех уровнях сети и проверяет все действия. Kaspersky Industrial CyberSecurity немедленно оповещает компанию о любых аномалиях в производственном процессе
- Защита на уровне АРМ и HMI
  - Вирусы, неслужебное ПО, внешние устройства
- Защита от сетевых атак
  - Несанкционированные сетевые подключения
  - Несанкционированные команды управления
  - Отклонения параметров процесса от заданных правил



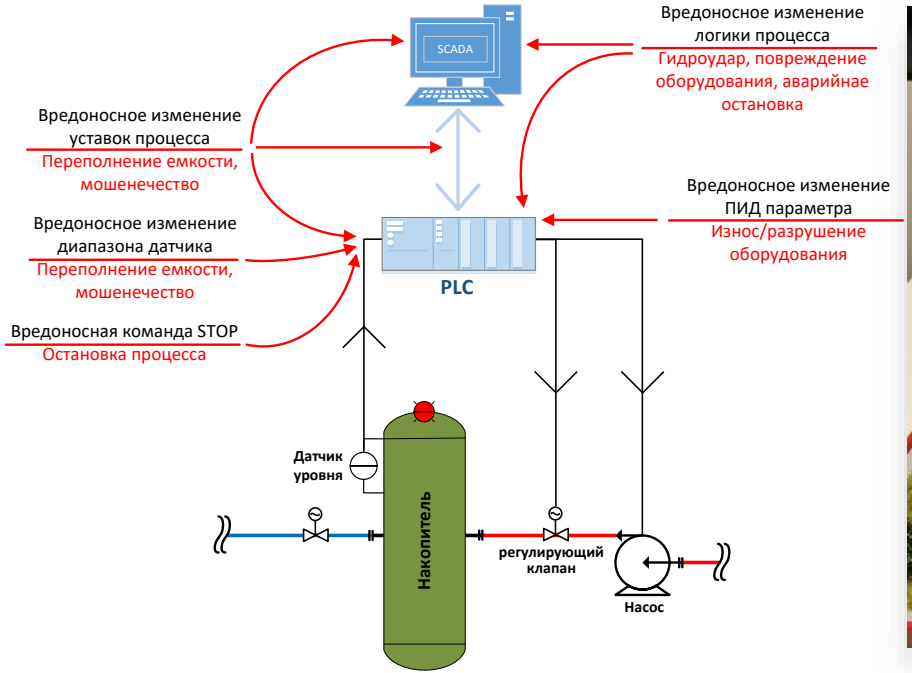
Результаты использования

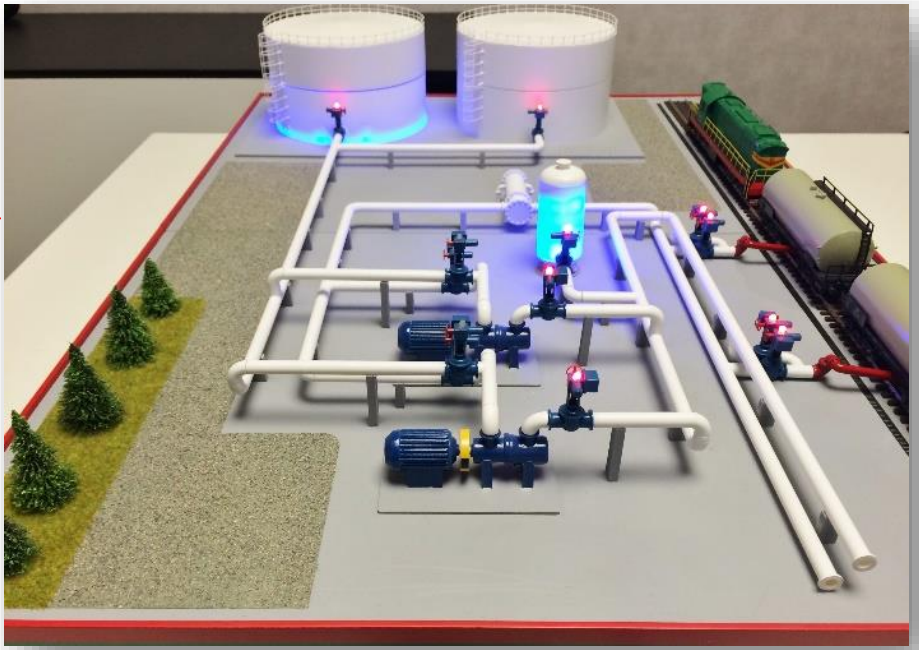
- Выявлены недостатки сегментации сети, посторонние коммуникации
- Отсутствие патчей уязвимых компонент и отсутствие практика регулярных аудитов
- Отсутствие процедур управления изменения конфигурации оборудования
- Избыточные сервисы расширяют поверхность атак
- Отсутствие отработанных процедур реагирования на инциденты

TANECO

- АО ТАНЕКО – современное предприятие нефтеперерабатывающей отрасли России, имеющее стратегическое значение для развития экономики Татарстана, входит в Группу компаний «Татнефть».
- ТАНЕКО стало первым за последние 30 лет масштабным инвестиционным и промышленным объектом, построенным на всём постсоветском пространстве с нуля. компания
- Задача провести обследование состояния информационной безопасности железнодорожной платформы по сливу вакуумного газойля и продемонстрировать возможность обеспечения кибербезопасности АРМ-операторов и SCADA-серверов, а также контроля целостности технологической сети и контроля ключевых параметров технологического процесса. В дополнение к этому предложенное решение не должно было оказывать никакого влияния на технологический процесс и не требовать изменения конфигурации АСУ ТП.

Векторы киберфизических атак





Результаты использования KICS

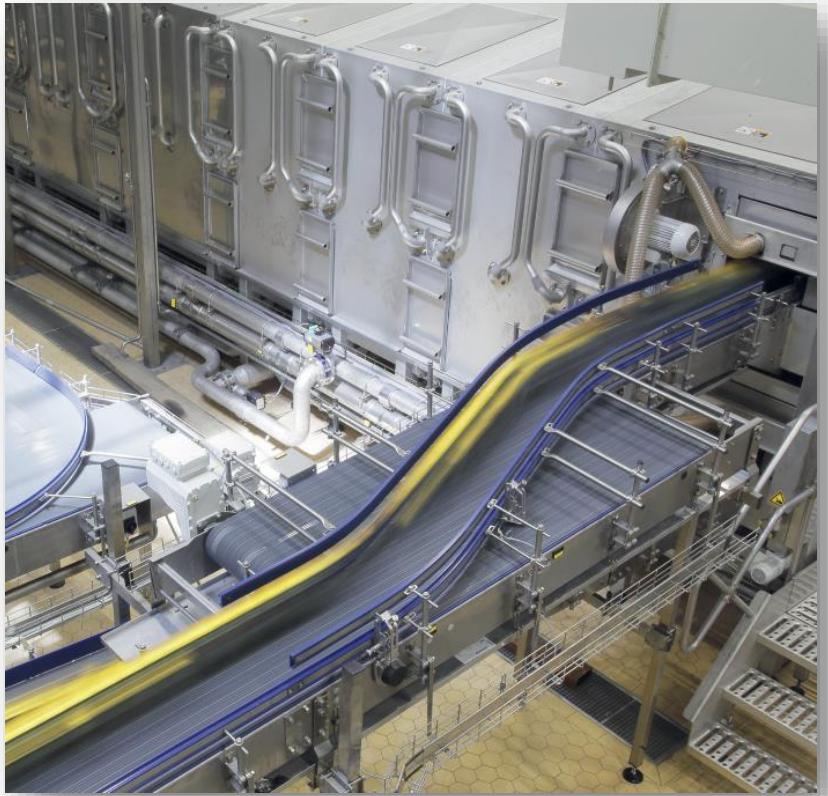
«Уже в первые месяцы работы решение по защите индустриальных объектов «Лаборатории Касперского» обнаружило несанкционированное подключение стороннего ноутбука к одному из контроллеров, а также попытку изменить параметры работы датчика».

Марат Гильмутдинов,
начальник отдела АСУ ТП,
АО ТАНЕКО

- Plzeňský Prazdroj – первая пивоваренная компания, начавшая производить светлое пиво низового брожения бренда Pilsner Urquell. Его оригинальная технология используется в производстве более чем двух третей выпускаемого сегодня в мире пива, в названии которого есть слово пилзнер, пилсенер или просто пилз. Название Plzeňský Prazdroj и Pilsner Urquell можно приблизительно перевести как «Подлинный источник Пилзнер».
- Plzensky Prazdroj – ведущая пивоваренная компания в Центральной Европе. Под своими брендами Plzensky Prazdroj продает больше пива на чешском рынке, чем любая другая компания. С 1999 года пивоваренный завод являлся частью группы компаний SABMiller (в то время «Южноафриканские пивоваренные заводы»). В 2017 году Pilsner Urquell (за исключением отдельных географических регионов) был продан Asahi, ведущему производителю пива и безалкогольных напитков в Японии

Завод

- Основные промышленные процессы в Plzeňský Prazdroj – пивоваренное производство и линии розлива. В общей сложности это 2 пивоваренных цеха, зоны цилиндроконических танков и 8 линий розлива на заводе в Пльзене
- Анализ защищенности для проверки инфраструктуры на завершающем этапе проекта по виртуализации промышленных систем и модернизации основных компонентов промышленной сети.
- Цель проекта по анализу защищенности заключалась в проверке надежности защиты от кибератак всех производственных линий и связанных с технологическим процессом программных и аппаратных средств, а также готовности компании к реализации целостной стратегии промышленной кибербезопасности



Результаты (обезличенные)

- Проблемы с сегментацией
- Избыточная функциональность
- Проблемы с паролями
- Проблемы физическим доступом
- Проблемы с регистрацией событий
- Избыточные права у пользователей
- Удаленный доступ
- …

TOP 30 IDENTIFIED WEAKNESSES IN FY 2016			
NIST 800-53 Weakness Categories	**Instances**	**Percentage**	**Order**
Boundary Protection	94	13.4%	1
Least Functionality	42	6.0%	2
Identification and Authentication (Organizational Users)	36	5.1%	3
Physical Access Control	28	4.0%	4
Audit Review, Analysis, and Reporting	26	3.7%	5
Authenticator Management	24	3.4%	6
Least Privilege	20	2.9%	7
Allocation of Resources	19	2.7%	8
Account Management	17	2.4%	9
Remote Access	16	2.3%	10
Security Awareness Training	16	2.3%	11
System Security Plan	15	2.1%	12
Flaw Remediation	15	2.1%	13
Information System Monitoring	15	2.1%	14
Security Impact Analysis	14	2.0%	15
Transmission Confidentiality and Integrity	13	1.9%	16
Baseline Configuration	12	1.7%	17
Contingency Plan	12	1.7%	18
Information System Backup	12	1.7%	19
Security Engineering Principles	12	1.7%	20
Information System Component Inventory	11	1.6%	21
Media Use	11	1.6%	22
Role-Based Security Training	10	1.4%	23
Configuration Change Control	10	1.4%	24
System Interconnections	9	1.3%	25
Configuration Settings	9	1.3%	26
Publicly Accessible Content	8	1.1%	27
Audit Events	8	1.1%	28
Incident Response Plan	8	1.1%	29
Protection of Information at Rest	8	1.1%	30
Total Discoveries Identified for Top 30 Weaknesses	550		
Total Discoveries Identified in FY2016	700		

Отзывы

«Решение о сотрудничестве с «Лабораторией Касперского» было принято нами легко по ряду причин. Мы высоко ценим их опыт в области обеспечения кибербезопасности промышленных систем, высокий профессионализм и комплексность их решения по сравнению с другими поставщиками. Всё это позволило создать благоприятные условия для развития целостной стратегии безопасности в нашей компании»

Ондрей Сикора,
менеджер C&A
Plzeňský Prazdroj

История продолжается