Барышников П.В. Развитие информационной безопасности на промышленных заводах: тренды и вызовы // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 9(35) с. 25–29

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

РАЗВИТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОМЫШЛЕННЫХ ЗАВОДАХ: ТРЕНДЫ И ВЫЗОВЫ

Барышников П.В.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: dedmars@bk.ru

В современном мире информационная безопасность стала одной из ключевых составляющих успешного функционирования промышленных заводов. Вмешательство в работу компьютерных систем, кибератаки и утечки конфиденциальной информации представляют серьезные угрозы для производства и, следовательно, для экономики в целом. Развитие информационной безопасности на промышленных заводах становится необходимостью для защиты критической инфраструктуры и обеспечения непрерывности производственных процессов.

Ключевые слова: Информационная безопасность, промышленные заводы.

DEVELOPMENT OF INFORMATION SECURITY AT INDUSTRIAL PLANTS: TRENDS AND CHALLENGES

Baryshnikov P.V.
BONCH-BRUEVICH ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS, St. Petersburg, Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail: dedmars@bk.ru

In the modern world, information security has become one of the key components of the successful operation of industrial plants. Interference in the operation of computer systems, cyber attacks and leaks of confidential information pose serious threats to production and, consequently, to the economy as a whole. The development of information security at industrial plants is becoming a necessity to protect critical infrastructure and ensure the continuity of production processes.

Keywords: : Information security, industrial plants.

Тренды в развитии информационной безопасность.

1. Интеграция ИТ и ОТ: С ростом автоматизации и цифровизации производственных процессов происходит объединение информационных технологий (ИТ) и операционных технологий (ОТ). Это создает новые уязвимости, требующие интегрированного подхода к информационной безопасности.

2. Использование искусственного интеллекта (ИИ) и машинного обучения (МО): Технологии ИИ и МО могут помочь в обнаружении аномалий в сетях и процессах, а также в прогнозировании потенциальных угроз.

3. Защита от внутренних угроз: Одним из важных аспектов является предотвращение и обнаружение внутренних угроз со стороны сотрудников. Системы мониторинга и анализа поведения пользователей (UBA) могут помочь в этом.

4. Разработка безопасных IoT-устройств: Промышленные IoT-устройства становятся все более распространенными. Их безопасность - ключевой аспект, так как они могут быть использованы как точка входа для кибератак.

5. Обучение персонала: Обучение сотрудников безопасности и всего персонала на заводе является важным фактором. Чем более информированными будут сотрудники, тем менее вероятность успешной кибератаки.

Вызовы перед промышленными заводами

1. Сложность сетей и систем: Промышленные заводы имеют сложные сети и системы, что делает сложным обеспечение безопасности каждого элемента. Необходимо иметь детальное понимание архитектуры и потенциальных уязвимостей.[1]

2. Неоднородность оборудования: Промышленные заводы могут использовать оборудование разных поколений, что усложняет внедрение единой системы безопасности.

3. Соответствие нормативам и стандартам: Заводы должны соблюдать множество нормативных требований и стандартов в области информационной безопасности, что требует значительных ресурсов.

4. Экономические ограничения: Инвестиции в информационную безопасность могут быть значительными, и заводы должны найти баланс между безопасностью и экономической эффективностью.[2]

Развитие информационной безопасности на промышленных заводах становится все более важным аспектом успешной деятельности. Требуется интегрированный подход, который включает в себя использование передовых технологий, обучение персонала, а также соблюдение нормативов и стандартов. Промышленные предприятия должны понимать, что инвестиции в безопасность - это не расход, а вложение в будущее, обеспечивающее стабильное и надежное производство.

Поддержание и развитие информационной безопасности на промышленных заводах - это процесс, который требует постоянного внимания и улучшения. Ниже представлены некоторые практические шаги, которые могут помочь заводам справиться с вызовами и продолжить развивать свои системы безопасности:

1. Аудит безопасности: Проводите регулярные аудиты и оценки уязвимостей в системах и сетях. Это поможет выявить слабые места и устранить их до того, как станут жертвами кибератак.

2. Мониторинг и реагирование: Внедрите системы мониторинга и реагирования на инциденты. Эффективное обнаружение и быстрое реагирование на угрозы помогут минимизировать потенциальный ущерб.

3. Обучение персонала: Проводите регулярные тренинги и обучение сотрудников по вопросам безопасности. Обеспечьте им знания и навыки для распознавания фишинговых атак и других угроз.

4. Политика доступа: Управляйте доступом к информации и системам, предоставляя разрешения только сотрудникам, которым это необходимо для выполнения их обязанностей.

5. Шифрование данных: Используйте шифрование для защиты конфиденциальных данных в покое и в движении.

6. Резервное копирование данных: Регулярно создавайте резервные копии важных данных и проверяйте их восстановление. Это поможет в случае утраты данных в результате атаки или сбоя систем.[3]

7. Обновление и патчи: Убедитесь, что все программное и аппаратное обеспечение на заводе обновлено и включает последние патчи безопасности.

8. Сотрудничество с экспертами: Рассмотрите возможность сотрудничества с внешними экспертами по информационной безопасности или фирмами, специализирующимися на киберзащите. Они могут предоставить экспертную поддержку и инсайды о текущих угрозах.

9. Управление рисками: Разработайте стратегию управления рисками в области информационной безопасности и периодически пересматривайте ее.

10. Соблюдение нормативов: Уделяйте внимание соблюдению секторальных и международных нормативов и стандартов по информационной безопасности.

Развитие информационной безопасности на промышленных заводах - это непрерывный процесс, который требует инвестиций времени, ресурсов и экспертизы. Однако это необходимо для обеспечения стабильной и надежной деятельности завода в условиях угроз и вызовов современного цифрового мира.

1. Инцидентный план: Разработайте и регулярно обновляйте инцидентный план. Этот план должен включать в себя четкие инструкции и процедуры для действий при возникновении киберинцидентов. Важно, чтобы весь персонал знал, как действовать в случае чрезвычайных ситуаций.

2. Изоляция сетей: Разделяйте сети на критические и не критические, и используйте различные уровни защиты для них. Это поможет предотвратить распространение атак на важные системы.

3. Анализ и учеба на опыте: После каждого инцидента проводите анализ произошедшего, чтобы понять его причины и последствия. Это позволит учиться на опыте и улучшать системы безопасности.

4. Социальная инженерия: Уделяйте особое внимание обучению сотрудников распознаванию социальной инженерии и фишинговых атак. Это одна из наиболее распространенных техник атаки.

5. Регулярные тестирования на проникновение: Проводите регулярные тесты на проникновение, чтобы оценить уровень защиты вашей системы. Эти тесты позволяют выявить уязвимости и устранить их до того, как их смогут использовать злоумышленники.

6. Создание культуры безопасности: Поддерживайте и развивайте культуру безопасности среди сотрудников. Убедитесь, что безопасность воспринимается как обязанность каждого сотрудника, а не только ИТ-специалистов.[4]

7. Информационное сотрудничество: Участвуйте в обмене информацией о киберугрозах с другими организациями в вашей отрасли. Это поможет узнавать о новых угрозах и обмениваться опытом.

8. Постоянное обновление стратегии: [5] Периодически пересматривайте и обновляйте стратегию информационной безопасности в соответствии с изменяющимися угрозами и технологическими трендами.

Заводы, инвестирующие в информационную безопасность, не только защищают свои активы и производственные процессы, но и поднимают свой уровень конкурентоспособности. Эффективная информационная безопасность - это необходимое условие для долгосрочного успеха в мире, где киберугрозы становятся все более хитрыми и серьезными. Помните, что безопасность - это процесс, а не конечная цель, и требует постоянного внимания и усилий.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018".–2018.–С.149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018.–2018.–С.31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).–2019.–С.590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».–2020.–№.2.–С.86-94.

References

1. Kotenko I. V. et al. Human-machine interaction model based on touch screens for monitoring the security of computer networks //Regional Informatics "RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: actual aspects of the"GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creation and management of Security Operations Center for effective application in real conditions //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St.

Petersburg State University"The Pragmatic Programmer: Your Journey to Mastery" by Andrew Hunt and David Thomas