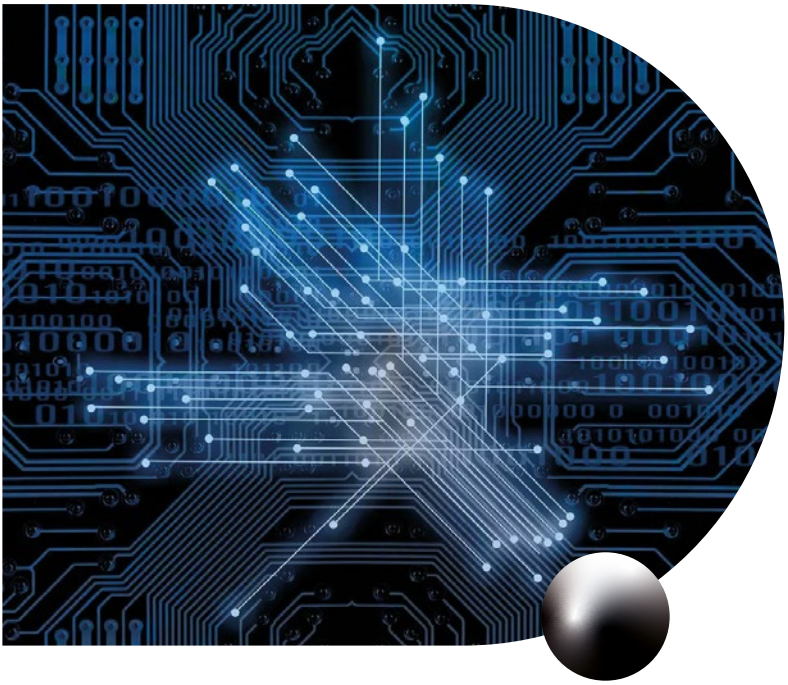
IT.Integrator

Перший в Україні проєкт побудови системи інформаційної безпеки АСУТП

Замовник: Об’єкт критичної інфраструктури

Галузь: Енергетика

Рішення: Система інформаційної безпеки АСУТП



Ця історія успіху зруйнує всі ваші попередні уявлення про кейси з IT індустрії, реалізовані в Україні, які ви мали змогу читати раніше. Цей проєкт – не просто про сучасні технології та промисловий розвиток, він є ще одним прикладом мужності, сили духу та наполегливості українців, адже, попри все, він не тільки був успішно завершений під час повномасштабної війни, а й отримав подальше масштабування на інші об’єкти та ліг в основу відбудови стандартів інформаційної безпеки цілої галузі.

Про замовника та передумови

У мирні часи навряд було б погоджено називати назву підприємства-замовника, тим паче, коли в країні вже більше року триває війна, а країна-терорист продовжує полювання на українські об’єкти критичної інфраструктури та провідні промислові майданчики. І це стосується не лише фізичного знищення, а й охоплює цілу низку інших ризиків, серед яких одне з провідних місць займають інформаційні та кібератаки.

Тому, згадуючи замовника, можемо визначити, що він відноситься до об’єктів критичної інфраструктури та захищає енергетичну незалежність України. Географія проєкту покрила чотири виробничі підрозділи на відстані від 30 до 130 км від центрального офісу компанії.

IT.Integrator

Перший в Україні проєкт побудови системи інформаційної безпеки АСУТП

Унікальність проєкту

- Тривалість зупинки виробництва під час впровадження — 0 хв.
- Архітектура - п’ятирівнева модель Purdue.
- Кількість співробітників інтегратора, задіяних у реалізації проєкту — більше 70 людей.
- Кількість співробітників замовника, задіяних у реалізації проєкту — менше 10 людей.

В основу передумов проєкту в першу чергу лягли послідовний розвиток інноваційності та технічної зрілості компанії-замовника. Важливий внесок зробили корпоративні рекомендації щодо зменшення ризиків втрати інформації та зупинки виробництва в разі кібератак та інцидентів. Зокрема, слід згадати постанову Кабінету Міністрів України N° 518 від 19 червня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури», що визначають організаційно-методологічні, технічні та технологічні умови організації кіберзахисту таких об’єктів. Зокрема, до технологічних новацій підштовхувала роками побудована система взаємодій, яка вимагала аудиту та систематизації згідно нової узгодженої архітектури, а вимога наявності документальних стандартів сприяла б уніфікації систем при будуванні нових об’єктів підприємства.

Склад рішення

Першочерговим завданням команди інтегратора стало забезпечення контролю доступу та контролю внесення змін до автоматизованих систем керування технологічними процесами. Другим пріоритетом було визначено забезпечення захисту АСУТП від кіберзагроз, своєчасне виявлення та попередження відмов обладнання. Як наслідок, для реалізації першочергових завдань, необхідно було модернізувати базову промислову інфраструктуру, побудувати відмовостійку систему кібербезпеки та реалізувати механізми проактивного захисту з використанням систем збору та аналізу журналів подій, виявлення аномалій та інцидентів кібербезпеки. Ще одним етапом стала розбудова захищеної та контрольованої демілітаризованої зони для обміну даними між промисловою та IT мережами. А також, важливо було забезпечити автономність кожного виробничого підрозділу в разі компрометації або виходу з ладу окремого виробничого підрозділу. Кінцевою метою мало стати забезпечення повної інтеграції та сумісності побудованого рішення з механізмами, програмними та апаратними комплексами існуючих систем, що також було реалізовано в процесі проєкту.

IT.Integrator

Перший в Україні проєкт побудови системи інформаційної безпеки АСУТП

Виробники, задіяні в інтеграції

Cisco, Fortinet, Check Point, McAfee, Trellix, Dell Technologies, Microsoft, ABB, Siemens, Allen-Bradley, Schneider Electric, Hewlett Packard Enterprise, Yokogawa, Phoenix Contact, Waterfall (Stronger Than Firewalls)

Результати

Локально-обчислювальна мережа

В рамках проєкту були здійснені налаштування та впровадження індустріальної мережевої інфраструктури на базі відмовостійкого протоколу швидкої збіжності Resilient Ethernet Protocol (REP) у зв'язку з Spanning-Tree Protocol (STP). А також впровадження технології DMVPN (IPSEC), і навіть резервного каналу з урахуванням мереж 3G/4G передачі даних телеметрії. Для забезпечення безпеки компонентів індустріальної мережі, відповідно до їх взаємодії між собою, був здійснений поділ існуючої продуктивної технологічної мережі на багаторівневу модель Purdue. Побудований новий план IP адресації з урахуванням нового дизайну мережі. На кожному об'єкті реалізоване мультивендорне інспектування та фільтрація трафіку між рівнями. А впровадження дизайну DMZ здійснено з урахуванням архітектури сервісів Microsoft.

Для реалізації централізованої системи моніторингу та керування мережевими пристроями використано рішення Cisco Prime Infrastructure.

Одностороння передача даних DataDiode

Застосоване в ході впровадження рішення Waterfall Unidirectional Security Gateway є унікальним, тому що воно забезпечує високий рівень безпеки завдяки фізичному розділенню сегментів мережі. Даний клас рішень використовується саме для вирішення задач безпечного обміну між сегментами промислової та корпоративної мереж на об'єктах критичної інфраструктури, наприклад, атомних станціях, промислових майданчиках, нафтовидобувних та нафтопереробних підприємствах тощо. Впроваджене рішення необхідне для безпечного обміну даними OPC Data Access між трьома виробничими майданчиками та головним офісом замовника, захищаючи технологічні мережі від зовнішніх загроз.

ТОВ "ІТ-ІНТЕГРАТОР" | marketing@it-integrator.ua | www.it-integrator.ua | тел.+380 44 538 00 69

Модернізація інженерної інфраструктури

Комплекс робіт по модернізації інженерної інфраструктури передбачав проведення аудиту існуючих ліній зв'язку та створення нових каналів передачі даних для повного дублювання критично важливих вузлів виробництва, а також забезпечення налаштування резервних каналів в автоматичному режимі. Проведене маркування ліній зв'язку згідно нового плану IP адресації. Забезпечене основне та резервне живлення існуючого та нового обладнання, а також максимальна утилізація наявної інфраструктури.

Захист від шкідливого програмного забезпечення

Застосування рішення класу Next Generation Antivirus дозволило впровадити централізовану систему захисту від шкідливого коду для технологічного обладнання, а саме: виробничих серверів, інженерних машин та панелей керування технологічними пристроями.

Зберігання даних

В ході проєкту впроваджено централізовану систему резервного копіювання та відновлення даних на підставі цільових рівнів відновлення критичних систем АСУТП згідно вимог RTO\RPO, які відповідають критеріям бізнесу замовника.

Віддалений доступ

У виробничих підрозділах була розгорнута служба віддалених робочих столів та впроваджено логічну структуру та топологію сайтів для мережевого середовища. Безпека віддаленого доступу була реалізована за рахунок впроваджених політик керування робочими станціями та серверами, а також матриці доступу до інформаційних ресурсів. Серед іншого, для забезпечення віддаленого доступу співробітників та підрядників впроваджені технічні рішення DNS, сертифікації, NTP, Terminal server.

Моніторинг інцидентів

Для моніторингу інцидентів та векторів атак була впроваджена єдина централізована система збору, аналізу та довгострокового зберігання журналів подій з усіх компонентів IT-інфраструктури – мережевого обладнання, підсистем захисту, серверів і робочих станцій – на базі рішення класу SIEM від Trellix.

Висновки

Валентин Герасимович, керівник проєкту «IT-Інтегратор»: *«Наша команда змогла реалізувати цей складний та багатошаровий проєкт, що охопив впровадження майже у всіх ланках інфраструктури замовника, починаючи від інженерної та закінчуючи надпотужними системами кібербезпеки. Попри початок повномасштабного вторгнення ворога в країну, ми успішно завершили всі поставки, монтаж, пусконалагодження обладнання, навчання персоналу та супровід замовника після впровадження. Більше того, ми змогли започаткувати стандарти, які в перспективі можуть бути застосовані на інші об'єкти, продовжуючи шлях продуктивної цифровізації процесів замовника».*

Надія Омельченко, віцепрезидентка «IT-Інтегратор» розповіла: *«Нами успішно реалізовано перший в Україні проєкт системи інформаційної безпеки автоматизованих систем управління технологічними процесами з використанням захищених однонаправлених мережевих пристроїв – датадіодів. Відпрацьовані таким чином підхід та технологію захисту відтепер можна впроваджувати та швидко масштабувати для всіх об'єктів критичної інфраструктури та підприємств стратегічних галузей промисловості, що гарантує 100% фізичний захист інформаційних систем такого об'єкту від вхідних кібератак».*