БАЗОВІ РЕКОМЕНДАЦІЇ З КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ СИСТЕМ

Практичний посібник для керівників та спеціалістів АСУ ТП промислових підприємств

Версія 1.0 від серпня 2017

Технічний комітет 185 "Промислова автоматизація"

БАЗОВІ РЕКОМЕНДАЦІЇ З КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ ДЛЯ ВІДДІЛІВ АСУ ТП

Версія 0.93 від серпня 2017

Призначення: цей документ містить базові рекомендації від Групи «Кібер-безпека» Технічного комітету 185 щодо першочергових та необхідних заходів протидії кібер-атакам в АСУ ТП. Документ призначений в першу чергу для керівників АСУ ТП промислових підприємств та інших об'єктів критичної інфраструктури, але буде корисний також всім керівникам та спеціалістам, задіяних в заходах по кібер-безпеці підприємств.

Фактори вразливості в АСУ ТП. Головні тенденції.

Нині в промислових системах керування спостерігаються дві тенденції: поступовий перехід засобів керування на стандарт Ethernet та протоколів TCP/IP і поява специфічного промислового шкідливого ПЗ, що атакує конкретні типи промислових систем керування. Ця тенденція в індустрії серйозно вплинула на пов'язаність процесів всередині систем керування в бік їх ускладнення. Побудова мереж АСУ ТП за принципом офісних мереж призвела до міграції вразливостей останніх в промисловий IT-контур. ПЛК та інші засоби керування польового рівня, разом з підключенням до Ethernet, стали відкриті до нових джерел загроз, на які їх розробники не розраховували. В результаті серйозно зросла кількість збоїв і простоїв обладнання через наслідки дії шкідливого ПЗ і кібератак. Це дві сторони однієї медалі. З одного боку, Ethernet-мережа, що пронизує собою наскрізь всі рівні підприємства, – це гнучкий і зручний інформаційний простір, що дозволяє вивести процеси автоматизації на новий рівень. З іншого боку, шкідливе ПЗ нового типу тепер може втрутитися в виробничий процес і нанести як великі матеріальні збитки діяльності самого підприємства, так і викликати катастрофічні наслідки з людськими жертвами.

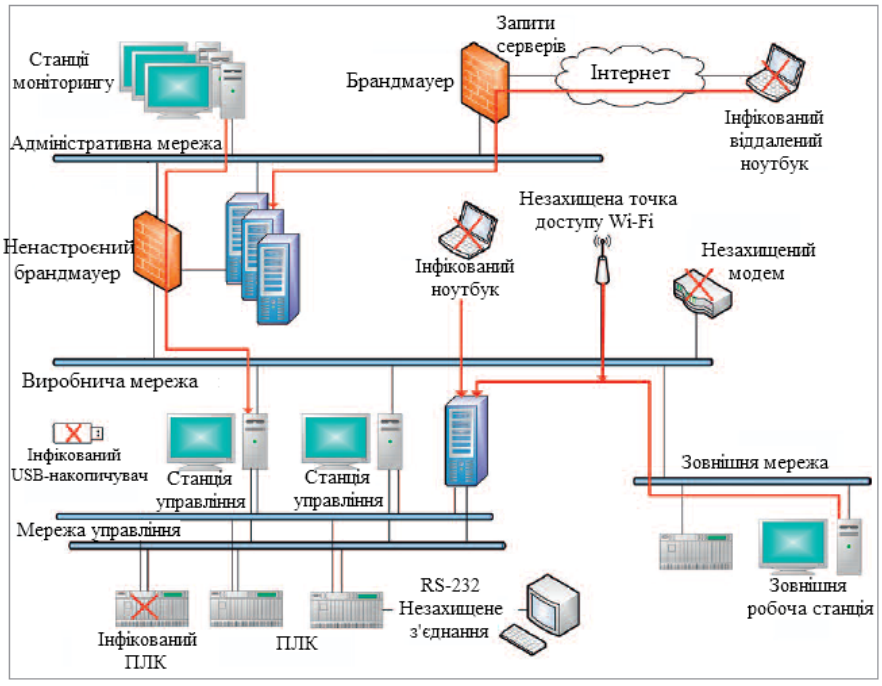

Рис. 1. Можливі шляхи проникнення шкідливого ПЗ в систему керування

На відміну від IT безпеки, що фокусується на захисті даних від крадіжки (таких як номери кредитних карток, корпоративна інформація тощо), головна мета заходів із кібер-безпеки системи керування – це підтримувати виробництво в робочому та безпечному стані. Основна загроза для обох цілей – це проникнення зловмисної програми до системи.

Зловмисне програмне забезпечення зазвичай інфікує систему через (Рис. 1):

- використання існуючих механізмів обміну для передачі файлів та віддаленного доступу до систем, наприклад надання загального доступу до файлів та протоколу передачі файлів (FTP);
- відкриття користувачем файлів, або запуск программ, що виглядають надійними, але мають не бажане ПЗ всередені;
- використання вразливостей у під'єднаному до мережі програмному забезпеченні, що дозволяє виконати вживляння зловмисного коду в систему;
- автоматичне копіювання файлів з портативних медіа, таких як USB-накопичувачі, CD, DVD та мобільних телефонів, до системи.

Такі фактори, у свою чергу, вимагають від інженерного складу відділів АСУ ТП підприємств прийняття ряду першочергових заходів для зменшення ризику проникнення до системи керування технологічними процесами на підприємстві шкідливого ПЗ та мінімізації можливих збитків у разі такого проникнення.

Дані рекомендації містять правила, дотримуючись яких, персонал відділу АСУ ТП здатний до деякої міри впоратися з цим завданням. Наведено 11 кроків, що їх потрібно пройти для захисту від цих загроз. Ці кроки запозичені із документів NIST, ISA 99 та інших стандартів з промислової кібербезпеки, що були інтегровані в один міжнародний стандарт МЕК 62443. Вони документують не тільки механізми кібербезпеки системи керування, але й вимоги до постачальника, що необхідні для посилення безпеки системи вже на об’єкті.

Наступні кроки виходять з піраміди автоматизації (Рис. 2) та вкладаються у концепцію, за якої необхідний рівень безпеки не може бути досягнутий одним лише придбанням системи керування із необхідним набором функцій забезпечення кібербезпеки. Вона стверджує, що **безпека це більше процес, ніж технологія.** Ці кроки спрямовані не лише на захист від дій зловмисного програмного забезпечення, але й від інших ризиків, що загрожують промисловим системам керування.Ці кроки можна виконувати у еволюційному стилі, послідовно підсилюючи безпеку із часом.

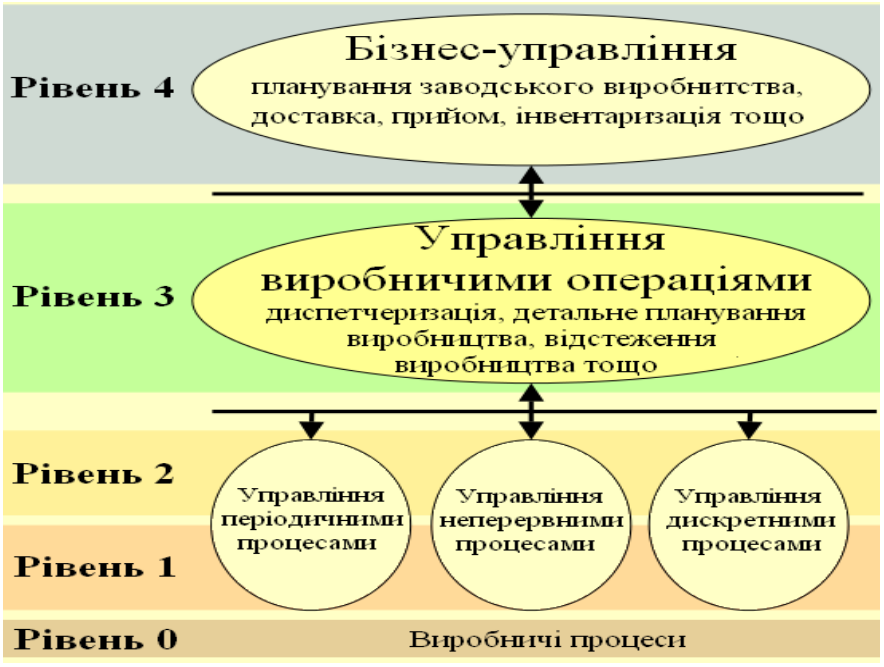

Рис. 2. Піраміда автоматизації згідно МЕК 62264

Крок № 1. Створення політик безпеки

Перш за все, необхідно впевнитись в існуванні політик безпеки для системи керування. Якщо вони відсутні для АСУ ТП їх можна запозичити з організаційних політик IT департаменту підприємства. Це буде перший крок на шляху до кібербезпеки OT. Ваші політики безпеки повинні будуть підтримувати кожен із наступних 10 кроків та бути спрямованими на захист Вашої системи від не авторизованого програмного забезпечення.

Крок № 2. Встановлення мережевих периметрів безпеки

Крок № 2 передбачає встановлення мережевих периметрів безпеки для обмеження точок доступу, де стороннє програмне забезпечення може увійти до системи керування. Як показано на піраміді автоматизації (Див. Рис. 2), у типовій системі керування підприємством корпоративні мережі відносяться до рівня 3 та вище, у той час як SCADA, мережі систем керування та польові шини відносяться до рівня 2 та нижче.

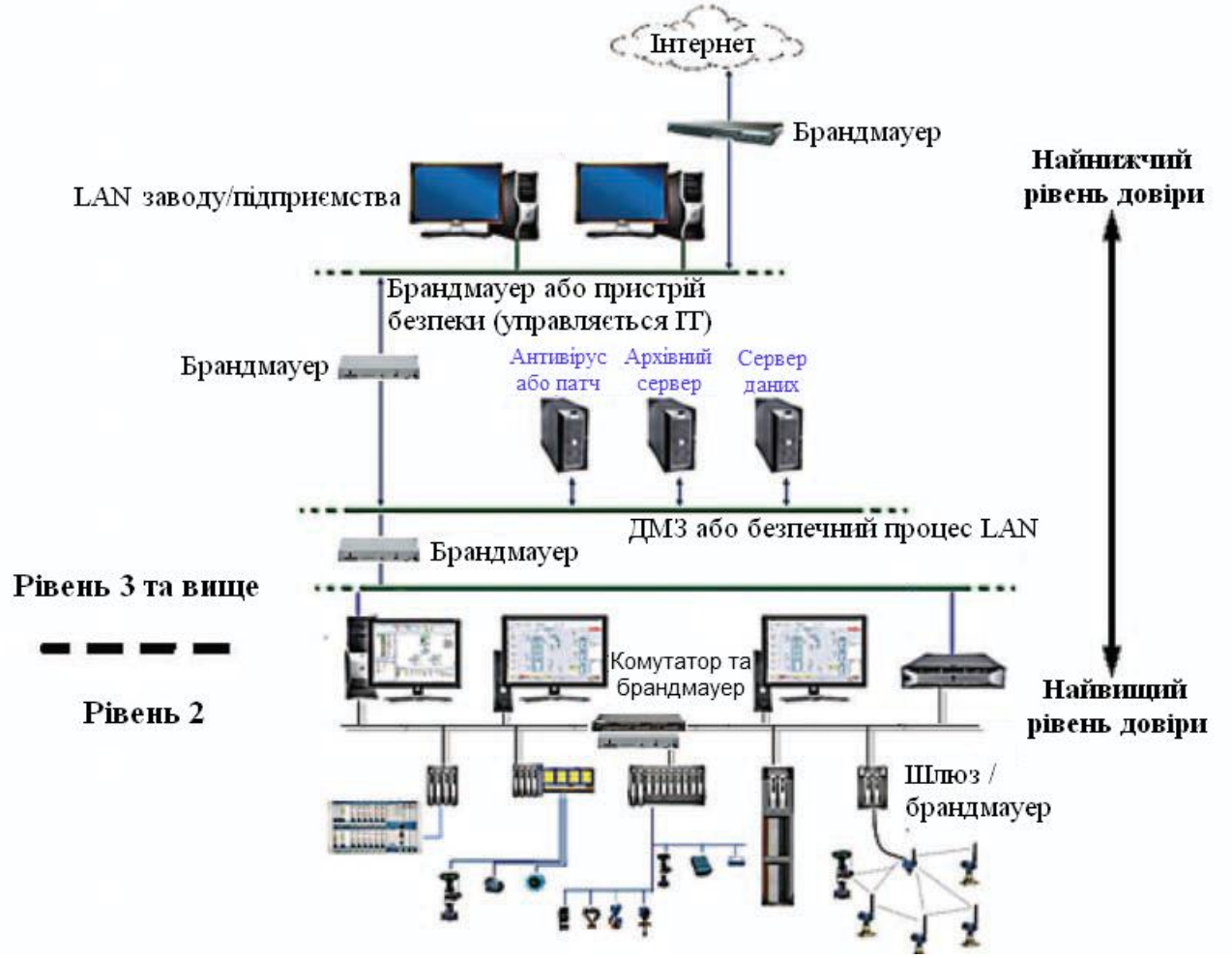

Рис. 3. Використання брандмауерів на рівнях піраміди автоматизації

Брандмауери використовуються для сегментації самої системи керування та ізоляції її від рівня 3 та інших зовнішніх мереж. **Необхідно бути упевненим, що весь трафік від і до системи керування шифрований та проходить принаймні через один брандмауер. За жодних обставин робоча станція рівня 2 не може мати прямого доступу до Інтернету або мати «білу» IP-адресу, що дозволяє їй бути безпосередньо досяжною із Інтернету.**

У складі системи керування брандмауери також слід використовувати для захисту контролерів, промислових бездротових мереж та мереж обладнання із категорії систем керування функціонально-небезпечними об'єктами від робочих станцій рівня 2. Крім того, **для попередження під'єднання сторонніх пристроїв до системи керування слід використовувати комутатори, що підтримують блокування портів.** Ці брандмауери та комутатори разом із брандмауерами рівня 2 та рівня 3 створюють шари периметрів безпеки із найнижчим ступенем довіри до рівня 3 та найвищим – до рівня 0.

Компоненти, що не є такими критичними для досягнення необхідних рівнів безпеки та доступності, такі як сервери архівних даних, повинні бути встановлені на вищому рівні ієрархії із меншим рівнем безпеки але із більшими можливостями до доступу, щоб у персоналу була можливість для перегляду та редагування даних.

Коли брандмауери та комутатори вже встановлені, вони потребують обслуговування протягом всього життєвого циклу системи для підтримання їх ефективності. Правила брандмауерів повинні актуалізуватись згідно зі змінами у IT-обладнанні та обладнанні системи керування для захисту від нових загроз. **Порти комутатора, що не використовуються, повинні регулярно перевірятися на предмет того, що вони заблоковані**.

Крок № 3. Захист робочих станцій

Крок № 3 передбачає захист робочих станцій систем керування у спосіб ускладнення шляху-проникнення зловмисного програмного до системи. Потрібно виконати дев'ять основних дій:

1. Необхідно впевнитись у повному впровадженні рекомендацій від IT-департаменту підприємства (Крок 1) на кожній робочій станції.
2. **Робочі станції повинні бути обмежені інженерними функціями і всі програми, служби та порти, що не потрібні для виконання цих функцій, повинні бути видалені або відключені**, щоб попередити використання відомих або ще не відомих уразливостей.
3. **Повинно бути встановлене спеціалізоване для промислових мереж антивірусне програмне забезпечення для виявлення та видалення відомого зловмисного програмного забезпечення до того, як воно інфікує робочу станцію.** Крім того антивірусні бази повинні підтримуватись у актуальному стані для того, щоб знаходити нові модифікації вірусів. Встановлювати на робочих станціях та серверах виробничої мережі та мережі управління антивірусне ПЗ загального призначення – **неприпустимо**!
4. По можливості, слід використовувати для запуску виконуваних програм «білі списки». Запуск усіляких інших програм повинен бути заборонений.
5. **При використанні шифрування в поштовому обміні слід використовувати локальний поштовий клієнт з додатковою перевіркою поштових відправлень локальною антивірусною програмою.** Це знижує можливість ураження комп'ютера вірусом з поштового вкладення.
6. Файлову систему слід конфігурувати таким чином, щоб тільки авторизовані користувачі мали доступ до критично важливих файлів. На жаль, по замовчанню, доступ до всіх файлів дозволений будь-якому користувачу із привілеями адміністратора. **Функціональні обов'язки користувачів повинні бути докладно проаналізовані та надано доступ тільки до тих файлів та каталогів, які їм дійсно потрібні.**
7. **USB-накопичувачі, CD та DVD-приводи слід заблокувати і використовувати тільки у дозволених випадках**. Блокування слід здійснити на рівні BIOSSetupадміністратором мережі. Користувачам потрібно нагадувати про те, що використання переносних медіа – це основний шлях інфікування системи. Користувачів слід ознайомити з організаційними засобами впливу за несанкціоноване використання переносних медіа та CD/DVD. Існують випадки, коли атакуючий залишає інфікований

USB-накопичувач на столі чи підлозі, сподіваючись, що хтось його підбере та підключить до своєї робочої станції. Ще один яскравий приклад недбалого відношення до безпеки зі сторони персоналу та керівництва підприємства є наступний: хоч робочі станції і відносяться до систем керування і практично всюди вони без доступу до Інтернету, але сусідній комп'ютер, «для пошти і т.і.» можуть випадково ввімкнути «тимчасово» в один комутатор, що і робоча станція оператора. Навіщо? Тому що і з того і з іншого комп'ютера іноді потрібно друкувати на один і той же мережевий принтер!

8. Ці дії можуть бути підсилені ще одною: по можливості, **періодично перезавантажуйте постійно працюючі робочі станції для захисту від тих типів зловмисного програмного забезпечення, що розташовується тільки в оперативній пам'яті.** Під час деяких типів атак використовується програмне забезпечення, що розміщується тільки в оперативній пам'яті і через це його важко виявити. Робочі станції, проти яких використовують такий тип атак, зазвичай працюють цілодобово у режими 24/7. Перезавантаження таких робочих станцій може видалити подібне зловмисне програмне забезпечення.
9. Система повинна бути спроектована таким чином, щоб **при виході з ладу обладнання робочих місць операторів система керування забезпечила продовження управління технологічним процесом**, до його безпечного завершення.
10. **Пульти керування робочих місць операторів критичних виробництв** (таких, як АЕС, нафтохімія тощо), з яких здійснюється введення керуючих завдань, не повинні мати стандартної комп'ютерної клавіатури, а **повинні забезпечуватися спеціалізованими клавіатурами**, оснащеними тільки необхідними функціональними клавішами.

Крок № 4. Управління обліковими записами користувачів

Крок № 4 цілком пов'язаний з обліковими записами користувачів. **Користувачам слід надавати тільки ті привілеї, що їм потрібні, їх паролі повинні бути достатньо довгими та використовувати комбінації як мінімум трьох із чотирьох елементів: великих та малих літер, чисел та спеціальних символів.** Обмеження повноважень користувачів може знизити можливості стороннього програмного забезпечення, що проникло на робочу станцію, використати привілеї користувача для виконання зловмисних дій, що є дуже поширеною технікою для зловмисного програмного забезпечення.

Використання складних паролів значно ускладнює атакуючому ПЗ процес підбору або зворотного інжинірингу пароля, якщо вони вже отримали доступ до системи. Крім того, політики використання паролів повинні передбачати періодичне оновлення паролів та неможливість повторного використання старих паролів (останніх трьох). Правильне використання паролів може захистити не тільки від зловмисного програмного забезпечення, що намагається отримати доступ до системи, а також від дій атакуючого, що має за мету увійти до системи.

Якщо зловмисний код працює у складі програми користувача та може отримати пароль адміністратора, тоді можливе використання цього пароля для підвищення повноважень зловмисного програмного забезпечення, або взагалі його запуск від імені адміністратора. Такі методи часто використовуються зловмисним програмним забезпеченнями для підвищення своїх привілеїв.

Крок № 5. Оновлення програмного забезпечення

Ідея, що лежить в основі цього кроку, **це своєчасне встановлення виправлень та оновлень, пов'язаних із безпекою як операційної системи так і для всього програмного забезпечення системи керування.** Ці виправлення дозволяють позбутися вразливостей, що можуть бути використані для інфікування програмного забезпечення. В Інтернеті можна знайти безкоштовні утиліти, за допомогою яких хакери можуть сканувати робочі станції на наявність вразливостей, а потім автоматично інфікувати зловмисним кодом, що дає доступ до **cmd.exe** або дозволяє хакеру завантажити та запустити свій код на робочій станції.

Так само, **виправлення та оновлення для робочих станцій слід спочатку перевіряти на ізольованій робочій станції**, щоб уникнути некоректної роботи програмного забезпечення після його оновлення. Сертифіковані виробники обладнання автоматизації повинні перевіряти всі виправлення, що стосуються безпеки, на сумісність із своїми продуктами.

Для успішного виконання оновлення ПЗ повинно використовуватися резервування програмних серверів (серверів ВВ, серверів застосунків,, історичних серверів, термінальних серверів). У той час, коли оновлюється ПЗ і перезавантажується відповідний основний апаратний сервер (або віртуальна машина в дата-центрі), продовжує роботу резервний апаратний сервер (або резервна віртуальна машина). Потім навпаки – онолюється резервний сервер, в той час як основний сервер продовжує роботу.

Порядок оновлення ПЗ на робочій станції (сервері або клієнті) повинен бути наступний:

1. Тестове оновлення ПЗ на окремій «машині-пісочниці».
2. Очікування та спостереження за «пісочницею» деякий час.
3. Оновлення ПЗ на сервері (апаратному або віртуальній машині) так, як описано вище.

Крок № 6. Резервування ПЗ та його відновлення

Крок № 6 передбачає **впровадження плану резервування та відновлення ПЗ**. **Всі резервні копії повинні знаходитися на окремому від робочої станції носії, який повинен зберігатися в окремому приміщенні, не пов'язаному з приміщенням цеху чи відділу, де встановлено робочу станцію**. Ефективний план дозволяє відновити конфігурацію інфікованої системи та її програмне забезпечення до стабільного (неінфікованого) стану. Сертифіковані виробники засобів автоматизації повинні мати стратегію резервування та відновлення, яка рекомендує коли і як відновити систему до стабільного стану, навіть якщо факт інфікованості не доведений. Це дуже важливо, оскільки зловмисне програмне забезпечення часто переховується від детектування і може залишатися неактивним до якогось часу.

Для відновлення роботоздатності ПЗ пісдя кібер-атак використовувати:

1) програмне резервування функціональноссті SCADA-систем, тобто резервування програмних серверів (серверів ВВ, серверів застосунків, історичних серверів, термінльних серверів);
2) віртуалізацію програмних серверів в дата-центрах підприємства.
3) Для підвищення відмовостійкості від кібер-атак використовувати усюди, де це можливо, тонкі термінальні клієнти (і відповідно термінальні сервери), що:
4) унеможливлює кібер-втручання на рівні операторських станцій (так як немає обміну даними між термінальним сервером і термінальними клієнтами);
5) дозволяє резервувати термінальні клієнти (за рахунок резервування термінальних серверів).

Крок № 7. Спостереження та оцінювання ризиків

Сьомий крок пов'язаний із **спостереженням за системою на предмет підозрілої активності та оцінюванням ризиків. Пакети програмного забезпечення з моніторингу системи безпеки перевіряють лог-файли робочих станцій, брандмауерів, комутаторів та інших пристроїв на наявність стороннього програмного забезпечення.** Деякі програмні продукти спостерігають за мережевим трафіком, а також за використанням процесору та оперативної пам'яті у пошуках аномалій. **За відсутності автоматизованих програм для спостереження необхідно в ручному режимі перевіряти лог-файли подій та мережевий трафік на наявність підозрілої активності, такої як несподіване збільшення мережевого трафіку, особливо у нетиповий час.**

Оцінювання ризиків слід проводити на етапі проектування, перед вводом у експлуатацію та протягом всього періоду експлуатації системи, щоб бути впевненим, що зміни у системі керування не призведуть до зниження її рівня безпеки. Дії, що можуть бути прийняті після оцінювання ризиків, можуть включати створення нових правил для брандмауерів, блокування портів у комутаторах, більш жорсткі політики для паролів, видалення програмного забезпечення, що не використовується, та покращення процедур по підключенню зовнішніх пристроїв, наприклад USB-накопичувачів.

Крок № 8. Ревізія всього використовуваного ПЗ

Необхідно провести ретельну ревізію всього використовуваного на робочих станціях програмного забезпечення на предмет виявлення несертифікованого ПЗ та ПЗ країни – агресора (Росія) та ПЗ компаній, що мають афілійований російський капітал. При наявності таких програм їх слід по можливості скоріше видалити з комп’ютерів та замінити на сертифіковані аналоги. Після цієї процедури слід провести нову повномасштабну перевірку системи для того, щоб бути упевненим, що в системі не залишилося зловмисних «закладок» від дій видаленого ПЗ.

Це необхідно для того, щоб виключити вже наявні закладки в російському ПЗ, які можуть вплинути на роботу системи керування обладнанням.

Крок № 9. Використання промислових контролерів та мережових пристроїв

Використовувати ПЛК з резервуванням керуючих мереж, тобто використовувати ПЛК з двома мережевими модулями, основний Industrial Ethernet або стандартний Ethernet, резервний – серіальний інтерфейс або стандартна польова шина. Використовувати в складі SCADA-систем програмне резервування комунікаційних серверів.

В промислових мережах Industrial Ethernet використовувати комутатори з протоколом контролю доступу до портів (протоколом аутентифікації станцій мережі) 802.1x.

Для об’єктів критичної інфраструктури рекомендується використовувати ПЛК з вбудованим протоколом контролю доступу до портів 802.1x і / або вбудованим протоколом симетричного блочного шифрування AES.

Обов’язковим є використання сертифікатів з підтримкою політики періодичної зміни сертифікатів.

Зміна паролів доступу до усіх пристроїв, підключених до мережі, повинна бути виконана з першого дня підключення. Залишати паролі пристроїв за замовчуванням – неприпустимо!

Крок № 10. Зонування (сегментування) промислової мережі

Зонування (сегментування) промислової мережі є ОБОВ'ЯЗКОВОЮ вимогою при реалізації нових систем керування технологічними процесами та модернізації вже існуючих. Без виконання вимог зонування мережі система керування ОТ не може бути прийнята до експлуатації.

Стандарт МЕК 62443 пропонує концепцію зон і каналів для сегментації та ізоляції ділянок і підсистем загальної системи управління. Зоною називається об'єднання логічних або фізичних засобів, для яких ставляться схожі вимоги з безпеки, наприклад, критичність для технологічного процесу. Устаткування в кожній зоні має певний рівень безпеки. Як правило, вбудовані засоби безпеки не задовольняють вибраного рівня, тому всередині зони застосовуються додаткові засоби і політики, що підвищують безпеку.

Весь обмін даними між зонами повинен бути взятий під контроль і проходити тільки по певним каналам зв'язку. Відстеження і аналіз трафіку, що проходить по виділених каналах, допомагає запобігти DoS-атаки і поширенню шкідливого ПЗ, захистити сусідні зони, цілісність і конфіденційність трафіку. В цілому контроль каналів зв'язку між зонами покликаний пом'якшити різницю між рівнями безпеки і вимог до неї. Забезпечення контролю таких каналів - набагато менш витратний захід, ніж модернізація кожного елемента всередині зони до досягнення відповідності заявленому рівню безпеки.

Таблиця 1. Ключові вимоги до зон і каналів зі стандарту МЕК 62443

Номер підрозділу і короткий опис	Вимоги
4.3.2.3.1. Розробка архітектури сегментованої мережі передачі даних	Кінцеві мережеві пристрої класифікуються відповідно до рекомендацій IASC (International Association of Classification Societies), кожен клас в залежності від рівня потенційної небезпеки відокремлюється в окрему захищену зону.
4.3.2.3.2. Ізоляція та сегментація обладнання з найбільш високим рівнем ризику	Зони з максимальним рівнем ризику повинні бути ізольовані за допомогою спеціальних бар'єрних пристроїв (промислових брандмауерів) від інших зон, що мають інший рівень чи інші політики безпеки. Бар'єрні пристрої підбираються відповідно з необхідним рівнем безпеки.
4.3.2.3.3. Блокування всіх невикористовуваних каналів зв'язку між зонами	Бар'єрні пристрої покликані блокувати весь недозволений трафік зони, що містить критично важливе обладнання, направлений як всередину зони, так і з захищеної зони назовні.

10.1. Зонування (Сегментування)

Сегментування мережі, виділення безпечних зон і каналів зв'язку між ними починається з групування устаткування за принципом схожої функціональності або вимог з безпеки. Виділені групи обладнання поділяються за зонами, для яких встановлюється певний рівень захисту.

Наприклад, апаратні засоби на першому етапі можуть бути розділені за виробничими зонами, такими як складські засоби автоматики, засоби АСУ основного технологічного процесу, засоби фінішної обробки продукції та інше. Потім всередині цих областей можлива подальша

сегментація за функціональними рівнями: MES-система, система операторського контролю (HMI), АСУ ТП (контролери ПЛК), система безпеки тощо. Іноді виділяються зони з обладнанням, які реалізують певний стандарт (МЕК 61850), або відповідно до рекомендацій виробника обладнання.

Кожна зона визначається набором атрибутів і характеристик. Ось деякі рекомендовані:

1. Характеристики зони:
   - назва зони;
   - визначення;
   - функціональна спрямованість.
2. Межі зони.
3. Типове обладнання (в ідеалі – перелік).
4. Ізоляція від інших зон.
5. Оцінка ризиків в межах зони:
   - можливості щодо забезпечення безпеки обладнання всередині зони;
   - загрози і уразливості;
   - наслідки виникнення «дірок» в системі безпеки;
   - можливий збиток від кібератак.
6. Мета забезпечення безпеки.
7. Стратегії забезпечення безпеки.
8. Застосування нових політик.
9. Обмін даними між зонами (вимоги до доступу).
10. Модифікація системи управління відповідно до попередніх змін.

Кожна зона визначається не тільки своїм периметром, набором засобів автоматизації і аналізом ризиків, але й можливостями щодо забезпечення безпеки. Наприклад, можливості з забезпечення безпеки в зоні, де використовуються сервери під управлінням ОС Windows 2008 Server, серйозно відрізняються від зони, де використовуються Windows NT або ПЛК. Відмінності в можливостях і в рівнях потенційних загроз породжують різні вимоги до систем безпеки самих зон і каналів зв’язку між ними. Визначити вимоги і потенційні можливості щодо забезпечення безпеки допоможе стандарт МЕК-62443.03.03: Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels («Безпека для систем автоматизації і керування. Вимоги до безпеки систем і рівні забезпечення безпеки»).

Зони також можуть виділятися відповідно до набору керуючого обладнання. Наприклад, ПЛК старого зразка мають слабші механізми авторизації, тому можуть бути виділені в окрему зону, де будуть додані необхідні функції перевірки користувачів.

10.2. Визначення захищеності з’єднувальних каналів між зонами

Після сегментування мережі передачі даних на зони наступним етапом є виділення зв'язків між зонами, в термінології стандарту – каналів. Кожен канал визначається згідно зонам, які він з'єднує, технологіям, які використовуються для зв’язку між зонами, протоколам передачі даних і функцій безпеки в цих зонах. Трафік, що проходить по таким каналам, як правило детально відомий. Утиліти-аналізатори трафіку і протоколів дають досить повну інформацію про обмін даними і про сервіси, що використовують канал.

Також корисно заглянути за мережу, виділити приховане переміщення даних. Наприклад, чи передаються файли між інженерною лабораторією і зоною, що охороняється, на USB-носіях? Чи трапляються віддалені підключення до терміналів всередині зони через модем? Такі «дрібниці» легко випустити з уваги, але разом з тим вони утворюють серйозний пролом в безпеці при відсутності уваги до них.

Діаграма руху даних (Див. Рис. 4) – відмінний інструмент для обліку даних в зонах і каналах між ними. Кожна зона може позначатися прямокутником, а рух певних даних – вектором.

Рис. 4. Приклад діаграми руху даних

10.3. Захист каналів зв'язку

Щойно канали зв'язку виділені і вимоги щодо забезпечення безпеки визначені, настає час застосовувати технології щодо забезпечення безпеки. Дві найбільш відомі з них наступні:

- брандмауери – це граничні пристрої, що контролюють і інспектують трафік в зону і з неї. Вони порівнюють трафік, що проходить через них, з заздалегідь закладеними в них політиками безпеки, і всі пакети даних, що не належать до дозволених типів – видаляються. Зазвичай вони конфігуруються на пропуск мінімального обсягу даних, достатнього для коректної роботи всієї системи. Особлива увага повинна приділятися трафіку з високим рівнем ризику, такого як команди програмування ПЛК або некоректно сформовані пакети даних, які можуть використовуватися для злому системи. Відмінності спеціальних промислових брандмауерів тут будуть очевидні: вони проектуються більше для інженерів АСУ ТП, ніж для IT-фахівців, і відповідно до потреб в АСУ ТП в них закладені можливості глибокого аналізу протоколів SCADA-систем, таких як DNP3, Ethernet / IP, ModBus TCP;
- мережі VPN (віртуальні мережі) – це зашифровані логічні канали зв'язку, що існують поверх фізичної мережі і реалізують приватну передачу даних та команд. Сесії VPN називають тунелями, вони реалізуються на третьому транспортному рівні моделі OSI, приватні дані передаються вкладеними в спеціальні пакети даних, видимі тільки зареєстрованим користувачам. Приєднання до мережі VPN здійснюється за допомогою спеціальних електронних ключів і сертифікатів.

Комплексний захист зон і каналів зв'язку можливий тільки при реалізації технологій захисту на всіх рівнях мережі, від фізичного до прикладного, що неможливо без спільної роботи фахівців відділів АСУ ТП і IT-відділів підприємства.

Крок № 11. Використання IIoT

Застосовувані технології IIoT на кожному рівні реалізації повинні використовувати:

- вбудовану безпеку (рішення на базі смарт-карт CardOS);
- захищені комунікації (модулі апаратного захисту і створення захищених ідентифікаторів);
- управління ідентифікаційною інформацією пов'язаних об'єктів (довірена інфраструктура);
- по можливості, не використовувати для критичних виробництв пристроїв з протоколом ZigBee. Рік назад його було зламано;
- використовувати https протокол всюди замість http. При цьому, обов'язково використовувати додатковий антивірусний захист контенту!;
- підтримку двофакторної авторизації;
- використовувати виключно серверну аутентифікацію, а не аутентифікацію на пристрої;
- використовувати виключно безпечні хмарні середовища.

Цифрові сертифікати гарантують повний захист при обміні інформацією за рахунок інтеграції ПЗ з сервісами аутентифікації, неможливості відмови від авторства і збереження конфіденційності.

На етапі впровадження IIoT слід:

- відрегулювати настройки конфігурації таким чином, щоб зменшити «площу дотику» з мережею;
- увесь код повинен виконуватися виключно від імені облікового запису з обмеженими правами;
- на приймаючій стороні в обов'язковому порядку перевіряти дані, що приходять від пристроїв користувачів;
- у якості пароля використовувати складні, недефолтні паролі;
- при роботі з обладнанням через WEB використовувати виключно протокол https.

Рекомендовані джерела

1. White Paper. Industrial Cybersecurity for Small- and Medium-Sized Businesses. A Practical Guide (2017)
2. White Paper. What Executives Need to Know About Industrial Control Systems Cybersecurity (2016)
3. NIST Special Publication 800-82 rev. 2. Guide to Industrial Control Systems (ICS) Security (2015)
4. Lee Neitzel. Intech. Six steps to control system cybersecurity (2013)
5. Байрс Э. Использование стандартов ANSI ISA-99 для обеспечения безопасности системы управления промышленным предприятием/Промышленные сети, №1-2014

Документ підготовлений в групі «Кібер-безпека» Технічного комітету 185 «Промислова автоматизація». Питанння, коментарі, відгуки – надсилайте на info@appau.org.ua