13. Кібербезпека промислових систем управління на основі комутованого доступу

Юлія Самойленко, Ярослав Смітюх, Олександр Мариненко
Національний університет харчових технологій, Київ, Україна

Вступ. Більшість промислових систем управління в даний час використовують операційну систему Microsoft Windows і промислову мережу Ethernet TCPJIP. Для забезпечення ефективного управління виробничими фондами використовується прямий зв'язок між системами управління та бізнес-процесами підприємства. Необхідно забезпечити кібербезпеку підприємства в цілому з метою збереження іміджу компанії та стабільності виробництва [1].

Методи досліджень. Багато промислових систем управління включають модем, який використовується як резервний, коли основна промислова мережа стає недоступною. Модеми являють собою, так званий “backdoor” для кібератак, який часто не помічають.

Результати і обговорення. Атака на промислові системи управління здійснюється за допомогою протоколу віддаленого терміналу (RTU) пристрою. Більшість RTU не використовують надійну аутентифікацію або інші механізми безпеки. Недоліком модему є прийом і відповідь будь-якого абонента. Цей факт дозволяє зловмиснику отримати доступ до мережі управління та промислової мережі. З точки зору поглибленого захисту, PBX (Private Branch Exchange) - це перше місце, де повинні розглядатися заходи безпеки. Для належної безпеки модему необхідно забезпечити функціонально схожі рівні безпеки між PSTN (Public switched telephone network) і компонентом системи керування. Однією з цікавих технологій є аутентифікація по телефону. За допомогою цієї технології апаратні ключі знаходяться на стороні модему загальнодоступної телефонної мережі (PSTN), а не між модемом і послідовним пристроєм, як це зазвичай робиться з пристроями вбудованого шифрування/аутентифікації, відомими в галузі як "зіткнення у дроті». Коли два телефони намагаються підключитися, головний ключ перевіряє підпорядкований ключ, перш ніж буде дозволено з’єднання PSTN. Якщо модеми проходять через систему PBX, яка не забезпечує належний рівень контролю, необхідний для досягнення цілей безпеки, розглядається можливість оновлення та/або використання телефонних брандмауерів між PSTN і модемом. Можна вважати, що цей тип апаратного забезпечення є еквівалентом корпоративного Інтернет-брандмауера для підключень PSTN. Він призначений для захисту голосової системи від «фрикерів», еквіваленту PSTN хакера. Деякі телефонні брандмауери включають можливість моніторингу трафіку телефонної лінії для виявлення зв'язку від внутрішніх модемів. Якщо модем не входить до списку авторизованих, брандмауер може автоматично заблокувати його, попередити про наявність неавторизованого модему. Ця здатність робить голосові брандмауери безцінними інструментами для виявлення неавторизованих модемів.

Висновок. Розглянуто способи забезпечення поглибленої безпеки промислових систем керування, яка необхідна модемам при побудові комутованого з’єднання при використанні пристроїв RTU.

Література

3. How can I...Reduce vulnerability to Cyber Attacks v3.0. (2019), *System technical note,* Schneider Electric.
4. Recommended Practice for Securing Control System Modems. (2008), *Homeland Security*, U.S. Department of Homeland Security.