УДК 004.056.57
Зайко Т.А.[1], Циммерман О.Г. [2]
[1] канд. техн. наук, доц. НУ «Запоріжка політехніка»
[2] студ. гр. КНТ-222м НУ «Запорізька політехніка»

ЕЛЕКТРОНІ ВИДИ ЗАГРОЗ У SCADA-СИСТЕМАХ

SCADA-системи є комп'ютеризованими системами управління, що призначені для моніторингу і контролю промислових процесів та критичної інфраструктури, такої як електростанції, водопровідні мережі та транспортні системи. Розвиток SCADA-систем зумовлений потребою у більш ефективному та інтелектуальному керуванні та моніторингу промислових процесів, а також зростаючим попитом на автоматизацію та оптимізацію. Однак забезпечення безпеки SCADA стає все більш важливим, оскільки системи стають більш підключеними та вразливими до кібератак та інших електронних загроз.

Однією з головних проблем SCADA-систем є вразливість цих систем до електроних видів загроз, насамперед до вірусів та кібератак, адже багато SCADA-систем мають застарілі програмні і апаратні засоби, які можуть бути легко скомпрометовані хакерами. Більшість SCADA-систем також підключаються до Інтернету, що сильно збільшує ризики.

Прикладом вразливості SCADA-систем до кібератак та вірусів став 2010 рік, коли відбулася масова кібератака на системи управління критичної інфраструктури за допомогою вірусу Stuxnet. Stuxnet використовував декілька вразливостей в SCADA-системах та промислових контролерах, що дозволило йому проникнути в систему та виконувати шкідливі дії. Одна з вразливостей, якою скористався Stuxnet, була пов'язана з протоколом зв'язку між комп'ютером оператора та контролером промислового обладнання. Вірус використовував цей протокол, щоб проникнути в систему та отримати доступ до контролера. Також вірус використовував підроблені цифрові підписи, щоб підміняти віруси та інші шкідливі програми на комп'ютерах операторів. Іншою вразливістю, якою скористався Stuxnet, була підтримка USB-накопичувачів в контролерах промислового обладнання. Вірус використовував цю вразливість, щоб передавати свій код на контролери через заражені USB-накопичувачі.

На прикладі захисту SCADA-систем від вірусу Stuxnet можна виділити основні існуючі у світі рішення для захисту SCADA-систем від вірусів:

– встановлення оновлень програмного забезпечення: Після того, як Stuxnet був виявлений, виробники ПЗ для контролерів промислового обладнання випустили оновлення програмного забезпечення, які попереджали атаки з використанням вразливостей, які були використані Stuxnet;

– зміна стандартних паролів: Stuxnet використовував стандартні паролі для залучення в системи і забезпечення себе надійним доступом. Зміна стандартних паролів на складні, унікальні і часто змінювані може захистити систему від атаки;

– встановлення брандмауерів: Брандмауери можуть захистити систему від атак, заблокувавши шкідливий трафік, який намагається проникнути в систему;

– шифрування трафіку: Використання шифрування для захисту трафіку, що передається між системами, може захистити його від перехоплення та відновлення інформації;

– організаційні заходи: Запровадження політик безпеки, які включають навчання персоналу про правильні методи безпеки, перевірку безпеки мережі та планування для можливих випадків кібератак, можуть допомогти зменшити ризик атак;

– використання систем виявлення вторгнень (IDS) і захисту від вторгнень (IPS) для моніторингу діяльності в мережі та запобігання незаконному доступу;

– використання антивірусів.

Більшість сучасних антивірусних програм мають сигнатури та евристичні алгоритми, які можуть виявити та блокувати як вірус Stuxnet, так і інші віруси, які можуть атакувати SCADA-системи. Однак, оскільки сучасні віруси і дуже складними та високорівневими, існує можливість, що деякі антивірусні програми можуть мати обмежену здатність виявляти їх.

Найкраще рішення для протидії вірусам - це використовувати сучасні антивірусні програми з актуальними сигнатурами та регулярно оновлювати їх, щоб забезпечити максимальний рівень захисту. Також важливо використовувати більш широку систему захисту, таку як брандмауер, IDS, IPS та інші системи безпеки, щоб забезпечити повний захист системи від можливих загроз.

Антивіруси можуть виявляти та блокувати Stuxnetта інші віруси, які здатні вражати SCADA-системи, використовуючи різноманітні методи. Найбільш часто використовуваними методами є сигнатурний аналіз, аналіз поведінки, евристичний аналіз.

Сигнатурний аналіз. Антивірусні програми можуть використовувати сигнатури шкідливих файлів, щоб виявити Stuxnet та інші шкідливі програми. Цей метод базується на порівнянні хеш-сум шкідливого файлу з хеш-сумами відомих вірусів, які зберігаються у базі даних антивірусної програми.

Аналіз поведінки. Антивірусні програми можуть аналізувати поведінку програм та процесів на комп'ютері, щоб виявити змінну поведінку, яка може свідчити про наявність шкідливої програми. Наприклад, Stuxnet може взаємодіяти з пристроями вводу-виводу, що може викликати підозру у антивірусної програми.

Евристичний аналіз. Антивірусні програми можуть використовувати евристичний аналіз, щоб виявляти нещодавно створені віруси, які ще не мають відповідних сигнатур. Цей метод може бути корисним для виявлення Stuxnet та інших сучасних вірусів.

Краще використовувати комбінацію різних методів виявлення та блокування вірусів для забезпечення максимального рівня захисту. Кожен з методів має свої переваги та обмеження, тому їхнє комбіноване використання може дати кращий результат.

Висновки.

Під час роботи у якості одної з головних проблем SCADA-систем було виділено їх вразливість до електронних видів загроз, а саме до вірусів. Цю проблему було показано на прикладі вірусу Stuxnet. В роботі було виділено основні існуючі у світі рішення для захисту SCADA-систем від вірусів. Було виділено найкраще рішення для протидії вірусам.Також було охарактеризовано основні методи протидії вірусам.