УДК 004.7.056.5(477)(045)

Олексій Юрійович Чередниченко
Віталій Вікторович Фесьоха
Юрій Олександрович Процюк
Тетяна Василівна Бондаренко

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ПРОТИДІЇ НАЙПОШИРЕНІШИМ КІБЕРНЕТИЧНИМ ВТРУЧАННЯМ В ІНФОРМАЦІЙНО–ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

Стрімкий розвиток інформаційно-комунікаційних технологій та Глобальної мережі Інтернет відкриває багато нових можливостей у всіх сферах життя людини і в країні загалом. З іншої сторони використання комп'ютерів, мобільних гаджетів та інших цифрових пристроїв сприяло розвитку нової загрози – кібернетичних втручань, під якими розуміють дії в кіберпросторі, спрямовані проти інформаційно-телекомунікаційної мережі метою впливу на неї шляхом порушення її функціонування, отримання контролю над мережею, корекції, копіювання, вилучення, пошкодження, впровадження чи знищення даних, створення умов для зміни поведінки її користувачів. В Україні в період з 2014 по 2017 роки відбулася низка кібернетичних втручань, які набули широкого розголосу як в країні так і в світі.

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. Тому доцільним буде проаналізувати найпоширеніші кібернетичні втручання, які були здійснені на території України та розглянути існуючі методи та способи попередження кібернетичних втручань, а також запропонувати метод та схему захисту від кібернетичних втручань.

Ключові слова: *кібернетичні втручання, кібератака, Firewall, IPS/IDS, кібербезпека, кібероборона.*

Вступ

За останні 4 роки Україна зазнала декількох масштабних кібернетичних втручань (далі – КВ) різного рівня складності та поширення. Більша їх частина була пов'язана із війною на сході України, яка розпочалась у 2014 р. Поява нових законів та прийняття нормативно-правових документів у сфері кібербезпеки держави обумовлює подальші дослідження та необхідність вирішення задачі підвищення ефективності кібербезпеки.

Аналіз сучасних кібератак в період з 2014 по 2017 роки показав слабкий рівень кібербезпеки в країні. За цей період їх жертвами були об'єкти енергетичної інфраструктури, Міністерства фінансів, Держказначейства, Пенсійного фонду. Було порушено роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ [1, 2].

Серед основних атак, які були здійснені на об'єкти критичної інфраструктури, можна виділити наступні: отруєння кешу DNS та розподілена атака на відмову в обслуговуванні (DDoS-атака), ефективної протидії яким на сьогоднішній день не створено.

Постановка проблеми. Залучення комп'ютерних технологій до все більшої кількості сфер діяльності держави, наближає Україну не тільки до світових стандартів та тенденцій, але й до їх негативних наслідків. Економіка, логістика та безпека країни все більше залежать від технічної інфраструктури та її захищеності. Для підвищення ефективності боротьби з КВ, доцільним буде проаналізувати найпоширеніші кібернетичні втручання, які були здійснені на території України та розглянути існуючі методи та способи попередження кібернетичних втручань, а також запропонувати надійний метод та схему захисту від кібернетичних втручань.

Аналіз останніх досліджень і публікацій [2 – 7] показав, що існує велика кількість методів та засобів захисту від такого роду КВ. До основних методів виявлення (протидії) належать такі, що побудовані на основі сигнатурного аналізу (методи виявлення зловживань) та методи виявлення аномалій. До основних засобів належать технології IPS/IDS, антивірусні програми, мережеві екрани (Firewall). Оскільки природа кібернетичних атак є різноманітною, тому не існує єдиного підходу до захисту від всіх кібератак одночасно. У зв'язку з цим, виникає завдання пошуку ефективного рішення виявлення (протидії) КВ в інформаційно-телекомунікаційні мережі (далі – ІТМ).

Метою статті є вибір ефективного методу захисту від КВ та способу застосування засобів попередження КВ.

Виклад основного матеріалу дослідження.

Методи захисту від кібернетичних втручань [2–5]. Існує дві основні групи методів аналізу подій в ІТМ для виявлення атак:

виявлення зловживань (misuse detection);

виявлення аномалій (anomaly detection).

Виявлення зловживань (сигнатурний метод). Детектори зловживань контролюють діяльність системи, аналізуючи подію або множину подій на відповідність заздалегідь визначеному зразку (сигнатурі), що описує відому атаку. Найбільш типова форма визначення зловживань, що здебільшого використовується у комерційних продуктах, визначає кожний зразок події, що відповідає атаці, як окрему сигнатуру. Проте існують складніші підходи для виявлення зловживань, що отримали назву технологій аналізу на основі стану (state-based), які можуть використовувати єдину сигнатуру для визначення групи атак.

Переваги й недоліки сигнатурного методу

Переваги сигнатурного методу:

детектори зловживань є дуже ефективними для визначення атак;

детектори зловживань не створюють величезного числа помилкових повідомлень;

детектори зловживань можуть швидко й надійно діагностувати використання конкретного інструментального засобу або технології атаки, це може допомогти адміністраторові скорегувати заходи для забезпечення безпеки;

детектори зловживань дозволяють адміністраторам, незалежно від рівня їхньої кваліфікації в області безпеки, почати процедури обробки інциденту.

Недоліки сигнатурного методу:

детектори зловживань можуть визначити тільки ті атаки, про які вони знають, необхідно постійно обновляти їхні бази даних для одержання сигнатур нових атак

більшість детекторів зловживань розроблені таким чином, що можуть використовувати тільки строго певні сигнатури, а це не допускає визначення варіантів загальних атак.

Виявлення аномалій. Детектори аномалій визначають ненормальне (незвичайне) поводження на хості або в мережі. Вони припускають, що атаки відрізняються від “нормальної” (законної) діяльності і можуть бути визначені системою, що здатна відслідковувати ці відмінності.

Детектори аномалій створюють профілі, що представляють собою нормальне поводження користувачів, хостів або мережних з’єднань. Ці профілі створюються, виходячи з даних історії, зібраних у період нормального функціонування. Потім детектори збирають дані про події й використовують різні метрики для визначення того, що аналізована діяльність відхиляється від нормальної.

Детектори аномалій і системи виявлення втручань (далі – СВВ), що на них засновані, часто створюють велику кількість помилкових повідомлень, тому що зразки нормального поводження користувача або системи можуть бути дуже невизначеними. Незважаючи на цей недолік, вважається, що СВВ, засновані на виявленні аномалій, мають можливість визначати нові форми атак, на відміну від СВВ, заснованих на сигнатурах, які цілком покладаються на відповідність зразку минулих атак.

Переваги й недоліки виявлення аномалій.

Переваги виявлення аномалій:

СВВ, засновані на виявленні аномалій, фіксують несподіване поводження і, таким чином, мають можливість визначити симптоми атак без знання конкретних деталей атаки;

детектори аномалій можуть створювати інформацію, що надалі буде використовуватися для визначення сигнатур для детекторів зловживань.

Недоліки виявлення аномалій:

виявлення аномалій звичайно створює велику кількість помилкових спрацьовувань про атаки при непередбаченому поводженні користувачів і непередбаченій мережній активності;

Виявлення аномалій часто вимагає деякого етапу навчання системи, під час якого визначаються характеристики нормального поводження. Від якості проведення цього навчання суттєво залежить подальша ефективність СВВ.

На основі аналізу розглянутих методів можна зробити висновок, що для підвищення рівня захищеності інформаційних ресурсів ІТМ доцільно застосовувати методи на основі виявлення аномалій, оскільки саме їм притаманно виявляти кібератаки 0-day (атаки нульового дня).

Основні засоби захисту від кібернетичних втручань. До основних засобів захисту від КВ відносяться: антивірусне програмне забезпечення; система запобігання/виявлення вторгнень IPS/IDS; мережеві екрани (Firewall). Типова схема застосування засобів захисту від КВ представлена на рис. 1.

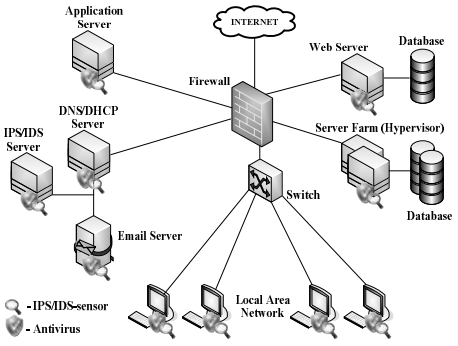

Рис. 1 Типова схема застосування засобів захисту від кібернетичних втручань.

Firewall (укр. мережевий екран) – це програма або обладнання, яке перешкоджає зловмисникам і

деяким типам шкідливих програм віддалено отримувати доступ до ІТМ. Для цього Firewall перевіряє дані, що надходять з Інтернету або по мережі, і розглядає їх на предмет блокування/дозволу передачі даних.

IDS/IPS (англ. Intrusion Detection System /Intrusion Prevention System, укр. Система виявлення вторгнення (СВВ)/Система запобігання втручання (СЗВ)). СВВ – програмний та/або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою.

Антивірусний захист – програмне забезпечення, яке здатне інтерактивно знаходити, протидіяти, блокувати, а також повністю видаляти віруси з системи.

Розглянута типова схема їх застосування (рис. 1) має суттєвий недолік: всі засоби працюють окремо та мають свою досить вузьку область застосування.

Технологія Cisco NG (next-generation) поєднує функціонал IPS та Firewall з метою покращення протидії КВ. Цей підхід себе виправдовує, проте, не включає весь спектр можливостей аналізованих засобів, що в свою чергу не надає повноможливого рівня забезпечення безпеки ресурсів сервісів ІТМ.

Тому пропонується до розглянутої схеми (рис. 1) додати координатор (рис. 2), основною метою якого буде координація дій всіх засобів. Координація функціонування цих засобів полягає в обміні командами управління та критичними даними в процесі аудиту подій в ІТМ.

Наприклад, у випадку ідентифікації IDS/IPS мережевої кібератаки на основі наявної аномалії в системі, брандмауеру надається команда від координатора на блокування ір-адреси підозрілої активності на основі даних, отриманих від IDS/IPS. В іншому випадку при наявності підозрілої активності без чіткої ідентифікації відправлення даного процесу у карантин для атаки, координатор надає команду управління антивірусному програмному забезпеченню для подальшого дослідження.

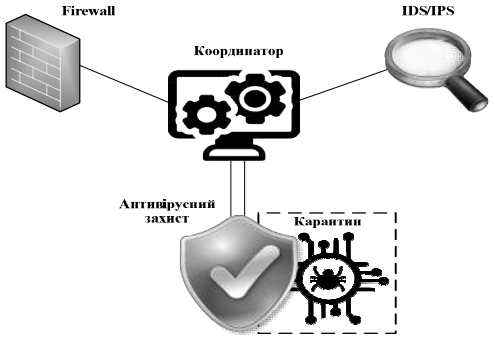

Рис. 2 Схема захисту від кібернетичних вторгнень з використанням координатора

Застосування такого підходу дозволить не тільки підвищити рівень кібернетичної захищеності ІТМ, а й може бути платформою для автоматичного створення експлойтів та сигнатур кібератак на основі наявних аномалій.

Висновки й перспективи подальших досліджень

Аналіз методів та засобів показав доцільність їх застосування до виявлення кібернетичних атак. Але наразі не існує єдиного універсального методу захисту від всіх видів атак в ІТМ. Запропонований у статті підхід передбачає застосування IDS/IPS методів на основі виявлення аномалій та включення до типової схеми застосування основних програмно та/або програмно-апаратних засобів захисту ІТМ модуля-координатора, що дозволяє значно підвищити рівень захисту ІТМ шляхом гібридизації їх функціоналу. Подальшим напрямком наукових досліджень може бути вибір конкретного методу на основі виявлених аномалій.

Література

1. Дрейс Ю.О., Мовчан М.С. "Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави", Актуальні питання забезпечення кібербезпеки та захисту інформації: третя міжнар. наук.-практ. конф., К.: Європейський університет, С. 71-74, 2017. **2. Субач І.Ю**. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій / І. Ю. Субач, В. В. Фесьоха, Н. О. Фесьоха. // Збірник наукових праць ІСЗЗІ. – 2017. – № 5 (1). **3. Басараб М.А.** Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов. // Вопросы кибербезопасности. – 2014. – №4 (5). – С. 30 – 40. **4. Kumar V.** Parallel and distributed computing for cybersecurity / V. Kumar //IEEE Distributed Systems Online. – 2005. – Vol. 6, №. 10. **5. Браницкий А. А**. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко. // Труды СПИИРАН. – 2016. – №45. – С. 207 – 244. **6. Feizollah A.** Anomaly Detection Using Cooperative Fuzzy Logic Controller / [A. Feizollah, S. Shamshirband, N. Anuar та ін.]. // Communications in Computer and Information Science. – 2013. **7. Ажмухамедов И. М.** Определение аномалий объема сетевого трафика на основе апарата нечетких множеств / И. М. Ажмухамедов, А.Н. Марьянков. // Вестник АГТУ. – 2011. – № 1 (51).

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ ПРОТИВОДЕЙСТВИЯ САМЫМ РАСПРОСТРАНЕННЫМ КИБЕРНЕТИЧЕСКИМ ВМЕШАТЕЛЬСТВАМ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ.

Алексей Юрьевич Чередниченко
Виталий Викторович Фесёха
Юрий Александрович Процюк
Татьяна Васильевна Бондаренко

Военный институт телекоммуникаций и информатизации имени Героев Крут, Киев, Украина

Стремительное развитие информационно-коммуникационных технологий и глобальной сети Интернет открывает много новых возможностей во всех сферах жизни человека и в стране в целом. С другой стороны использование компьютеров, мобильных гаджетов и других цифровых устройств способствовало развитию новой угрозы - кибернетических вмешательств, под которыми понимают действия в киберпространстве, направленные против информационно-телекоммуникационной сети с целью воздействия на нее путем нарушения ее функционирования, получения контроля над сетью, коррекции, копирования, удаления, повреждения, внедрения или уничтожения данных, создания условий для изменения поведения пользователей. В Украине в период с 2014 по 2017 годы прошел ряд кибернетических вмешательств, которые получили широкую огласку как в стране так и в мире.

В условиях глобализации информационных процессов, их интеграции в различные сферы общественной жизни руководство ведущих государств мира уделяет повышенное внимание созданию и совершенствованию эффективных систем защиты критической инфраструктуры от внешних и внутренних угроз кибернетического характера. Поэтому целесообразным будет проанализировать распространенные кибернетические вмешательства, которые были совершены на территории Украины и рассмотреть существующие методы и способы предупреждения кибернетических вмешательств, а также предложить метод и схему защиты от кибернетических вмешательств.

Ключевые слова: *кибернетические вмешательства, кибератака, Firewall, IPS/IDS, кибербезопасность, кибероборона.*

ANALYSIS OF EXISTING APPROACHES TO COUNTER THE MOST COMMON CYBERNETIC INTERVENTIONS IN INFORMATION AND TELECOMMUNICATIONS NETWORK

Oleksiy Y. Cherednychenko
Vitaliy V. Fesokha
Yurii O. Protsiuk
Tetyana V. Bondarenko

Military Institute of Telecommunications and Informatization named after Heroiv Krut, Kyiv, Ukraine

The rapid development of information and communication technologies and the global Internet opens up many new opportunities in all spheres of human life and in the country as a whole. On the other hand, the use of computers, mobile gadgets and other digital devices has contributed to the development of a new threat - cybernetic interventions, which are understood as actions in cyberspace directed against the information and telecommunications network with the aim of influencing it by disrupting its functioning, gaining control over the network, copy, delete, damage, insert or destroy data, create conditions for changing user behavior. In Ukraine, from 2014 to 2017, a number of cybernetic interventions were carried out, which were widely publicized both in the country and in the world.

In the context of the globalization of information processes and their integration into various spheres of public life, the leadership of the leading states of the world pays special attention to the creation and improvement of effective systems for protecting critical infrastructure against external and internal cyber threats. Therefore, it will be expedient to analyze the widespread cybernetic interventions that have been carried out on the territory of Ukraine and to consider existing methods and methods of preventing cybernetic interventions, as well as to offer a method and scheme for protection from cybernetic interventions.

Key words: *cybernetic interventions, cyberattack, firewall, IPS/IDS, cybersecurity, cyberdefense.*

References

1. Dreys Y.O., Movchan M.S. "Analysis of the negative effects of cyber attacks on information resources of critical infrastructure of the state", Topical issues of cyber security and information security: third international. science-practice Conf., K .: European University, pp. 71-74, 2017. **2. Shubach I.Y.** Ananalysis of existing decisions to prevent intrusion in information and telecommunication networks open on the basis of public licenses / I. Yu. Zubach, V.V. Fesoha, N.O. Fesioha. // Collection of scientific works of the Institute for Scientific Research. - 2017 - No. 5 (1). **3. Basarab M.A.** Detection of anomalies in information processes on the basis of multifractal analysis. Basarab, I.S. Stroganov. // Issues of cybersecurity. - 2014. - No. 4 (5). - P. 30 - 40**.**

4. Kumar, V. Parallel and distributed computing for cybersecurity / V. Kumar //IEEE Distributed Systems Online. – 2005. – Vol. 6, №. 10. **5. Branitsky A.A.** Analysis and classification of methods for detecting network attacks / A.A. Branitsky, I.V. Kotenko. // Proceedings of SPIIRAS. - 2016. - No. 45. - P. 207 - 244. . **6. Feizollah A.** Anomaly Detection Using Cooperative Fuzzy Logic Controller / [A. Feizollah, S. Shamshirband, N. Anuar та ін.]. // Communications in Computer and Information Science. – 2013. **7. Azhmukhamedov I.M.** Determination of anomalies in the volume of network traffic on the basis of an apparatus of fuzzy sets / IM Azhmukhamedov, A.N. Mariyankov. // Bulletin of the Astrakhan State Technical University. - 2011. - No. 1 (51).