КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.226237
УДК 004.057.2

Дудикевич Валерій Богданович
доктор технічних наук, професор,
професор кафедри захисту інформації
Національний університет «Львівська політехніка», м. Львів, Україна
ORCID ID: 0000-0001-8827-9920
vdudykev@gmail.com

Гарасимчук Олег Ігорович
кандидат технічних наук, доцент,
доцент кафедри захисту інформації
Національний університет «Львівська політехніка», м. Львів, Україна
ORCID ID: 0000-0002-8742-8872
oleh.harasymchuk@gmail.com

Партика Андрій Ігорович
кандидат технічних наук,
старший викладач кафедри захисту інформації
Національний університет «Львівська політехніка», м. Львів, Україна
ORCID ID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Совин Ярослав Романович
кандидат технічних наук, доцент,
доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

Нємкова Олена Анатоліївна
доктор технічних наук, професор,
професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», м. Львів, Україна
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

ДОСЛІДЖЕННЯ ПЕРЕВАГ ЗАСТОСУВАННЯ МЕТОДУ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ З ВИКОРИСТАННЯМ ВІРУСІВ-ВИМАГАЧІВ

Анотація. Дана стаття присвячена дослідженню і аналізу недавніх кібератак на об'єкти критичної інфраструктури України з використанням вірусів-вимагачів. У статті автори наголошують на зростанні важливості кібербезпеки у сучасному цифровому середовищі у зв'язку із зростанням кількості кіберзлочинів, зокрема, атак за допомогою вірусів-вимагачів. Внаслідок цього, важливим є застосування стандартів аудиту з кібербезпеки для ефективної протидії цим загрозам. Стаття підкреслює важливість впровадження комплексних заходів, які охоплюють технічні, організаційні та правові аспекти, для протидії кіберзлочинам з використанням вірусів-вимагачів. У статті також наведено основні способи і засоби для успішної протидії вірусам-вимагачам, як для звичайних користувачів, так і представників бізнесу та об'єктів критичної інфраструктури. Також, дана стаття пропонує дослідження переваг перехресного впровадження стандартів аудиту з кібербезпеки в контексті боротьби з кіберзлочинами, що використовують віруси-вимагачі. Автори розглядають методи та підходи до аудиту кібербезпеки, визначають переваги методу перехресного впровадження

стандартів та пропонують рекомендації щодо його ефективного використання для забезпечення безпеки інформаційних систем. Такий підхід сприяє створенню комплексної системи захисту, яка зменшує ймовірність успіху атак з використанням вірусів-вимагачів і забезпечує більшу стійкість організації до інцидентів та кіберзлочинів. Результати дослідження можуть бути корисними для організацій, що прагнуть покращити свою кібербезпеку та захистити себе від кіберзлочинів з використанням вірусів-вимагачів.

Ключові слова: інформаційна безпека, кібербезпека, об'єкти критичної інфраструктури, система управління інформаційною безпекою, стандарт кібербезпеки, кіберзлочин, віруси-вимагачі, інформаційні системи, ISO 27001, комп'ютерні мережі, моніторинг безпеки, SIEM, аудит кібербезпеки.

ВСТУП

У світі сучасних технологій, де високотехнологічні системи є необхідною складовою інфраструктури, загрози кібербезпеці стають все більш небезпечними і критичними. Масштаби та наслідки кібератак на критичну інфраструктуру демонструють необхідність ефективних заходів захисту. Порушення безпеки в галузях, таких як енергетика, транспорт та фінанси, можуть мати серйозні наслідки для економіки, соціальної стабільності та безпеки громадян. Забезпечення надійного захисту цих об'єктів є ключовим завданням, яке вимагає комплексного підходу та використання передових технологій [1].

Дослідження останніх резонансних атак на критичну інфраструктуру з використанням вірусів-вимагачів є критично важливим для розуміння сучасних загроз та розвитку відповідних заходів захисту. Порушення безпеки в цих секторах може мати далекосяжні наслідки, що варто уникнути за будь-яку ціну. Тому дослідження таких атак та методів їх протидії стає запорукою надійного захисту критичної інфраструктури в майбутньому.

Окрім того, вивчення цих атак може допомогти розробити кращі практики та стратегії захисту, які можуть бути застосовані в широкому спектрі галузей та інфраструктур. Це означає, що результати такого дослідження матимуть користь не лише для конкретних секторів, але й для загальної кібербезпеки.

Постановка проблеми. Для ефективного захисту об'єктів критичної інфраструктури необхідно використовувати передові технології та методики кібербезпеки. Стандарти аудиту з кібербезпеки надають систематичний підхід до виявлення потенційних загроз і впровадження заходів для їх запобігання. Вони допомагають організувати процес забезпечення безпеки, встановлюючи загальноприйняті рамки та вимоги [2].

Разом з тим, впровадження вимог стандартів аудиту з кібербезпеки в організаціях стикається з рядом проблем, таких як недостатня узгодженість між різними стандартами, велика кількість контролів та вимог, недостатність практичного досвіду у людей відповідальних за впровадження, а також складність їхнього впровадження та оцінки. Ці чинники можуть ускладнювати процес забезпечення відповідності та вимагати значних зусиль та ресурсів [3].

Таксономія загроз критичної інфраструктури є дуже широкою, і проблематикою даної статті не є охоплення всіх можливих векторів атак. Натомість, дослідження зосереджене на аналізі останніх резонансних атак на критичну інфраструктуру з використанням вірусів-вимагачів, а також методах протидії цим атакам.

Аналіз останніх досліджень і публікацій.

Вірус-вимагач – це вид шкідливого програмного забезпечення, який використовується кіберзлочинцями для вимагання коштів у жертв. Зазвичай, програма-вимагач блокує екран пристрою жертви або шифрує дані на диску, відображаючи вимогу про викуп із реквізитами платежу [4].

Вперше програма-вимагач була виявлена в 1989 році. Шкідлива програма отримала назву AIDS Trojan. Вона поширювалася через тисячі дискет, які містили інтерактивну базу даних про СНІД і фактори ризику, пов'язані з хворобою. Після запуску шкідлива програма фактично робила неможливим доступ користувача до більшої частини вмісту на диску. AIDS Trojan вимагав викуп в розмірі $189, які потрібно було надіслати на поштову скриньку в Панамі. Програма була запущена 365 разів. Автором загрози був доктор Джозеф Попп, однак його було визнано непідсудним [5].

У більшості випадків програма-вимагач відображає на екрані повідомлення, що ваш комп’ютер заблокований, або додає текстовий файл (повідомлення) до відповідних папок. Багато сімейств вимагачів також змінюють розширення зашифрованих файлів [6].

Оператори програм-вимагачів використовують багато різних технік інфікування:

- Шифрування диску та блокування доступу користувача до операційної системи;
- Блокування екрану користувача;
- Шифрування даних на диску жертви;
- Блокування пристроїв Android шляхом зміни коду доступу для заблокування пристрою користувача [7].

Усі перераховані вище види програм-вимагачів вимагають викуп, найчастіше у Bitcoin або в іншій криптовалюті. Натомість оператори загрози обіцяють розшифрувати дані або відновити доступ до інфікованого пристрою [8]. Однак немає ніякої гарантії, що кіберзлочинці виконають свою обіцянку (а іноді вони не можуть це зробити навмисно або через некомпетентне кодування).

На сьогодні, віруси-вимагачі є одними із найпоширеніших видів шкідливого програмного забезпечення в світі. Зокрема, вторгнення Росії в Україну посилило занепокоєння щодо інцидентів безпеки, а атаки програм-вимагачів стали реальною загрозою для компаній у всьому світі [9]. Зловмисники-вимагачі часто націлені на великі компанії або компанії, які зберігають конфіденційні дані. Такі компанії зазнають значних грошових збитків і репутаційних втрат для бізнесу [10].

Мета статті. Метою статті є аналіз останніх резонансних атак на критичну інфраструктуру з використанням вірусів-вимагачів, та розробка практичних рекомендацій для протидії кіберзлочинам з використанням вірусів-вимагачів.

Завдання. Для успішного досягнення мети статті необхідно виконати наступні завдання:

- Провести дослідження і аналіз недавніх атак на критичну інфраструктуру України з використанням вірусів-вимагачів шляхом збору та аналізу актуальних даних та статистики щодо інцидентів кібербезпеки.
- Провести дослідження щодо найкращих практик у сфері кібербезпеки для захисту і протидії атакам з використанням вірусів-вимагачів.
- Розробити рекомендації для звичайних користувачів і бізнесу для захисту від атак з використанням вірусів-вимагачів.
- Провести огляд та дослідити основні переваги використання методу перехресного впровадження стандартів аудиту з кібербезпеки для захисту об’єктів критичної інфраструктури від вірусів-вимагачів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд недавніх резонансних атак на критичну інфраструктуру України з використанням вірусів-вимагачів

Україна стала ареною для численних кібератак, спрямованих на критичну інфраструктуру, і використання вірусів-вимагачів у цих атаках не є винятком. Нижче наведено декілька недавніх прикладів атак на критичну інфраструктуру України з використанням вірусів-вимагачів [11].

Атака на енергетичну систему (2015). У грудні 2015 року в Україні сталася перша в історії кібератака, яка призвела до відключення електроенергії в деяких районах країни. Хакери використали вірус-вимагач BlackEnergy для атаки на комп'ютерні системи енергетичних підприємств.

Російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України. Наступна, і набагато менш масштабна за наслідками, кібератака сталась вночі з 17 на 18 грудня 2016 року. Протягом трохи більше однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берегу Києва та прилеглих районів області.

Найбільше від першої кібератаки постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом трьох-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж відбувалося з підмереж глобальної мережі Інтернет, що належать провайдерам в Російській Федерації.

Загалом кібератака мала комплексний характер та складалась щонайменше з таких складових:

- попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;
- захоплення управління АСДУ з виконанням операцій вимикань на підстанціях;
- виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, комутатори);
- знищення інформації на серверах та робочих станціях (утилітою KillDisk);
- атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Перерва в електропостачанні склала від 1 до 3,5 годин. Загальний недовідпуск — 73 МВт·год (0.015 % від добового обсягу споживання України).

Внаслідок другої кібератаки, в грудні 2016 року, струм був відсутній протягом трохи більше однієї години.

Petya та повідомлення про замінування (2017-2019). 27 червня 2017 року Україна зіткнулася з масштабною кібератакою, що вразила підприємства та установи різних форм власності. Її здійснили за допомогою шкідливої програми Petya, яка мала різні назви та асоціювалася з групою TeleBots, пов’язаною з відомим угрупуванням BlackEnergy-Sandworm. Метою атаки було повне знищення даних, що свідчило про наміри саботажу та демонстрації сили.

Технічна складність атаки полягала у застосуванні різноманітних інструментів та методів, як-от бекдори, інструменти для шифрування даних, а також способи горизонтального поширення у мережах через використання вразливостей, як-от EternalBlue, та інструментарій, як-от Mimikatz, PsExec та WMIC. Джерелом зараження була система оновлень бухгалтерської програми M.E.Doc, що свідчить про використання легітимного програмного забезпечення як засобу для поширення вірусів. У системі оновлень M.E.Doc виявили бекдори та вразливості, що сприяло поширенню атаки.

У жовтні 2017 року відбулася ще одна кібератака, відома як BadRabbit. Спочатку вона не привернула увагу, однак згодом з'ясувалося, що ця атака слугувала прикриттям для більш складної операції проти систем «1С» в Україні.

У 2018-2019 роках Україна стала свідком хвилі масових псевдозамінувань, інформація про які надходила з території РФ. Ці повідомлення були частиною інформаційної війни і демонстрували використання кіберпростору не тільки для технічних атак, але й для впливу на громадську думку та створення атмосфери страху.

Початок повномасштабного вторгнення (2022). У січні 2023 року фахівці Держспецзв'язку та експерти Ради економічної безпеки України провели дослідження кореляції комп'ютерних атак із політичними подіями та ракетними обстрілами від лютого до листопада 2022-го року.

Дослідження відстежило чітке узгодження ракетних ударів з кібератаками. Основними мішенями були медіа, центри зв'язку, інституції, які допомагають Україні, логістичні та енергетичні підприємства.

Хронологія деяких атак [12]:

січня 2022 року – Атаки на державні та банківські сайти. Приблизно 22 державні органи та 70 українських сайтів були атаковані з дефейсом, що засуджує український націоналізм. Атака була спрямована на залякування та можливе компрометування Польщі, хоча мала ознаки російського походження.

- 15 лютого 2022 року – Масштабна DDoS-атака. Сайти майже 15 банків і держорганів були недоступні протягом п'яти годин, що оцінювалося як найбільша кібератака в історії України.
- 23-24 лютого 2022 року – Атаки напередодні повномасштабного вторгнення. Масштабна кібератака порушила супутниковий доступ до інтернету. Хакери відключили модеми, які зв'язуються із супутником KA-SAT компанії Viasat, що забезпечують доступ до інтернет для клієнтів у Європі, зокрема в Україні. Відбулися атаки на державні та банківські сайти, а також на інші важливі інфраструктурні об'єкти, спричинені вірусом HermeticWiper. Атаки були спрямовані на підготовку до військового вторгнення.
- 8 квітня 2022 року – Кібератака на об'єкти енергетики України. За словами українських чиновників, атака мала початися ввечері 8 квітня, коли люди поверталися додому з роботи, і могла унеможливити їхнє повсякденне життя або мати наслідком отримання доступу до інформації про перебіг війни. Якби атака була успішною, вона позбавила б електроенергії приблизно 2 млн. людей і ускладнила б відновлення електропостачання.
- 13 травня 2022 року – Масова кібератака на мережі львівської мерії. Під час кібератаки на мережі мерії викрали частину робочих файлів міста та опублікували її на ворожих телеграм-каналах.
- 23 червня 2022 року – Російські спецслужби атакували сервер електронної пошти Миколаївської ОДА. Внаслідок цього вони отримали доступ до поштової скриньки пресслужби облдержадміністрації.

– 1 липня 2022 року – Кібератака на IT-інфраструктуру групи ДТЕК. Це кібератака на найбільшу приватну енергетичну компанію України, яку здійснили разом із ракетними ударами по Криворізькій електростанції.

Від 2023 року атаки ворога стають більш інтрузивними. У липні 2023 року урядова команда з кібербезпеки CERT-UA зафіксувала збільшення активності російського хакерського угруповання Armageddon. Група займалася кібершпигунством щодо сил безпеки й оборони України та здійснювала атаки на об'єкти інформаційної інфраструктури.

Підконтрольні спецслужбам РФ хакери також почали використовувати шпигунське ПЗ для стеження за мобільними пристроями бійців ЗСУ. За останній рік СБУ виявила щонайменше сім таких програм, зокрема Infamous Chisel для атаки на Android-пристрої.

У 2023 році російські хакери посилили атаки на українські правоохоронні структури. Зокрема, щоб отримати доступ до даних про докази воєнних злочинів РФ, запитів на затримання підозрюваних агентів тощо.

Від лютого 2022 року відбулося орієнтовно 10 тис. кібератак та критичних інцидентів, які зафіксувала лише СБУ. Це 10-15 спроб здійснити щось серйозне щодня, і кібератаки стали більш витонченими.

У січні 2023 року хакери активізували фейкові розсилки «запитів» від M.E.Doc — програми, яку широко використовують в українських держустановах та приватних компаніях для надання звітності. Листи містили файли-архіви, запуск вмісту яких призводить до зараження комп'ютера шкідливими програмами RemcosRAT та QuasarRAT, що дозволяють злочинцям отримати дистанційний контроль.

Ці атаки підкреслюють необхідність ефективного захисту критичної інфраструктури від вірусів-вимагачів, оскільки їхні наслідки можуть бути надзвичайно серйозними і призвести до значних збоїв у роботі інфраструктури.

Основні методи протидії вірусам-вимагачам

Захист користувачів. Орієнтований на дані період створює все більше проблем, пов'язаних із безпекою, з якими навіть експерти навряд чи можуть легко впоратися. Однією з найскладніших загроз є віруси-вимагачі/віруси-шифрувальники, які дуже важко виявити і ще важче вчасно заблокувати.

Основні правила для захисту власних даних та пристроїв від програм-вимагачів:

– Регулярне створення резервних копій даних та збереження принаймні однієї повної резервної копії.
– Оновлення програмного забезпечення, включно з операційною системою.
– Використання надійного антивірусного програмного забезпечення та регулярні сканування системи для виявлення та видалення потенційно шкідливих програм.
– Уникання відкриття непідтверджених або сумнівних посилань у електронних повідомленнях, електронній пошті, повідомленнях в соціальних мережах та інших джерелах.
– Установка програм лише з офіційних джерел та уникання скачування програм з ненадійних джерел.
– Увімкнення мережевого екрану на вашому пристрої та налаштування його на блокування непотрібного мережевого трафіку.

- Налаштування складних та унікальних паролів для кожного облікового запису і використання двофакторної аутентифікації, де це можливо.
- Уважне використання публічних Wi-Fi мереж та уникання введення конфіденційної інформації у незахищених мережах.
- Забезпечення фізичної безпеки пристроїв та уникання їхнього залишення без нагляду в громадських місцях.

Дотримуючись цих правил, ви можете максимально зменшити ризик зараження вашої системи шкідливим програмним забезпеченням.

Захист бізнесу та критичної інфраструктури. Бізнес та об'єкти критичної інфраструктури є особливо привабливими цілями для програм-вимагачів через їх значний вплив на економіку, громадську безпеку та нормальне функціонування суспільства. Захист від програм-вимагачів для цих суб'єктів є критично важливим.

Для бізнесу, а особливо для об'єктів критичної інфраструктури, необхідно вживати комплекс заходів кібербезпеки, які охоплюють технічні, організаційні та правові аспекти. Це включає в себе розробку та впровадження стратегій забезпечення безпеки, регулярні аудити безпеки, оновлення програмного та апаратного забезпечення, навчання персоналу з питань кібербезпеки, впровадження систем моніторингу та виявлення вторгнень, а також співпрацю з правоохоронними органами та іншими суб'єктами галузі.

Важливо також регулярно оцінювати загрози та ризики, а також вживати заходів для їхнього управління та мінімізації. Оскільки програми-вимагачі постійно еволюціонують і змінюються, бізнесам та об'єктам критичної інфраструктури слід залишатися завжди пильними та готовими до викликів кібербезпеки, надійно захищаючи свої системи та інформацію від потенційних загроз.

Нижче наведено основні правила для захисту бізнесу та об’єктів критичної інфраструктури від програм-вимагачів:

–**Вимкнення або видалення непотрібних сервісів та ПЗ**: Періодично переглядайте програми та сервіси, які використовуються в вашій системі, і видаляйте ті, які не є необхідними або є потенційно небезпечними.

–**Сканування мереж на наявність незахищених облікових записів:** Використовуйте спеціальні програми для автоматичного сканування мережі на вразливості та слабку автентифікацію, та ідентифікуйте облікові записи, які потребують покращення безпеки.

–**Обмеження або заборона використання RDP за межами мережі або вмикання аутентифікації на рівні мережі:** Встановлення обмежень на віддалений доступ до системи та вимагання додаткової аутентифікації для доступу до критичних ресурсів.

–**Використання VPN:** Застосовуйте VPN для шифрування з'єднання та захисту даних під час з'єднання з віддаленими мережами.

–**Перегляд параметрів брандмауера:** Регулярно аналізуйте і налаштовуйте правила брандмауера для блокування небажаного трафіку та захисту мережі від зовнішніх загроз.

–**Перегляд політики для трафіку між внутрішньою та зовнішньою мережами (Інтернет):** Перевірте та налаштуйте правила пропуску трафіку, щоб уникнути небажаного обміну даними між внутрішньою мережею та Інтернетом.

–**Встановлення пароля у налаштуваннях рішення безпеки:** Додайте пароль для захисту налаштувань системи безпеки, щоб запобігти незаконному доступу та втручанню.

–**Забезпечення захисту резервних копій за допомогою багатофакторної аутентифікації:** Використовуйте додаткові заходи безпеки, такі як багатофакторна аутентифікація, для доступу до резервних копій даних.

–**Регулярне проведення навчання персоналу для розпізнавання фішинг-атак та інших технік кіберзлочинців:** Організуйте тренінги та навчання для працівників щодо розпізнавання та запобігання кібератакам, включаючи фішинг.

Отже, захист бізнесу від програм-вимагачів стає все більш важливим у сучасному цифровому світі, де кіберзлочинці постійно шукають нові шляхи доступу до цінної інформації. Комплексний підхід до цього завдання передбачає вживання різноманітних заходів з кібербезпеки, оскільки жоден захід не може гарантувати повний захист.

Це включає в себе не лише технічні заходи, такі як встановлення антивірусного програмного забезпечення чи налаштування брандмауера, але й організаційні заходи, такі як навчання персоналу з питань кібербезпеки та розробка політик безпеки в компанії. Важливо також звернути увагу на аспекти управління ризиками, ідентифікацію вразливостей і розробку планів реагування на можливі інциденти.

Додатково, регулярне оновлення програмного забезпечення і здійснення аудитів безпеки допоможе запобігти використанню вже відомих вразливостей зловмисниками. Постійне вдосконалення стратегій та заходів захисту, відповідь на нові загрози та виявлення нових можливостей для покращення безпеки – це ключові аспекти успішної стратегії кібербезпеки для будь-якого бізнесу.

Перехресне впровадження стандартів аудиту з кібербезпеки

Перехресне впровадження стандартів аудиту з кібербезпеки, таких як ISO 27001, PCI DSS і NIST, для дослідження і протидії кіберзлочинам з використанням вірусів-вимагачів, є критично важливим кроком у забезпеченні безпеки інформаційних систем і має ряд істотних переваг (Рисунок 1).

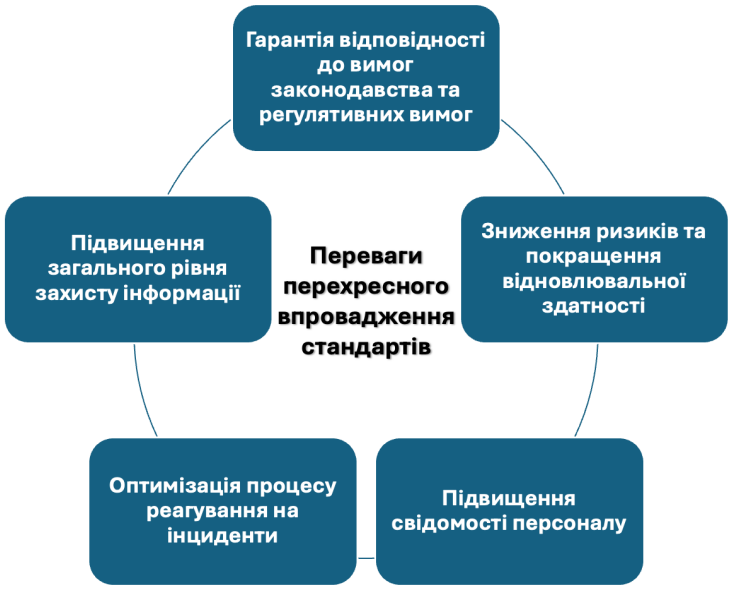

Рис. 1. Основні переваги перехресного впровадження стандартів аудиту з кібербезпеки

Ось кілька основних переваг такого підходу:

- **Гарантія відповідності до вимог законодавства та регулятивних вимог:** Стандарти, такі як PCI DSS, можуть встановлювати конкретні вимоги щодо захисту конфіденційної інформації, включаючи заходи проти вимагачів. Дотримання цих стандартів може допомогти вам уникнути санкцій і штрафів.
- **Підвищення загального рівня захисту інформації в організації:** Стандарти кібербезпеки, такі як ISO 27001 і NIST 800-53, визначають рекомендації щодо ефективних практик захисту інформації. Впровадження цих стандартів може допомогти підвищити рівень захисту вашої організації від атак вірусів-вимагачів.
- **Зниження ризиків та покращення відновлювальної здатності:** Аудит кібербезпеки з використанням стандартів, таких як ISO 27001 чи NIST, може допомогти ідентифікувати слабкі місця в вашій інфраструктурі та процесах, що сприяє зменшенню ризиків атак вірусів-вимагачів. Планування заходів для відновлення після атаки також є ключовим елементом стратегії безпеки, побудованої на основі таких стандартів.
- **Підвищення свідомості персоналу:** Впровадження стандартів кібербезпеки може сприяти підвищенню свідомості персоналу щодо потенційних загроз та заходів безпеки, що можуть допомогти уникнути атак вірусів-вимагачів.
- **Оптимізація процесу реагування на інциденти інформаційної безпеки:** Реагування на інциденти відіграє ключову роль у боротьбі з атаками з використанням вірусів-вимагачів. Використання стандартів аудиту кібербезпеки може допомогти вашій організації побудувати ефективний план реагування на інциденти та забезпечити швидке відновлення роботи систем після атаки.

Усі ці підходи сприяють створенню комплексної системи захисту, яка зменшує ймовірність успіху атак з використанням вірусів-вимагачів і забезпечує більшу стійкість організації до інцидентів та кіберзлочинів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дана стаття аналізує недавні резонансні атаки на об’єкти критичної інфраструктури України із використанням вірусів-вимагачів, і надає практичні рекомендації щодо протидії цим атакам.

Захист бізнесу від програм-вимагачів важливий через те, що програми-вимагачі можуть завдати серйозної шкоди даним та інфраструктурі, порушити роботу компанії, а також викликати значні фінансові і репутаційні втрати. Однак, із появою все більш складних загроз кібербезпеці, захист від програм-вимагачів вимагає комплексного підходу.

Застосування комплексу заходів кібербезпеки дозволяє забезпечити більш високий рівень захисту, оскільки різні заходи можуть взаємодоповнюватися та підсилювати один одного. Наприклад, вимкнення непотрібних сервісів та програм може зменшити вразливість системи, а сканування мережі на наявність слабких облікових записів допоможе попередити несанкціонований доступ.

КІБЕРБЕЗПЕКА: освіта, наука, техніка № 2 (22), 2023
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
ISSN 2663 - 4023

Додатково, використання стандартів/фреймворків кібербезпеки, таких як ISO 27001, PCI DSS, NIST, дозволяє створити систематичний підхід до керування кібербезпекою в організації. Ці стандарти аудиту надають набір рекомендацій та керівництво для створення, впровадження та підтримки ефективної програми безпеки. Вони допомагають організаціям ідентифікувати ризики, встановлювати прийнятні рівні безпеки та розробляти плани для запобігання та реагування на інциденти кібербезпеки. Такий систематичний підхід дозволяє забезпечити ефективний захист від широкого спектру кіберзагроз.

Загалом, комплексний підхід до захисту бізнесу від програм-вимагачів не лише забезпечує ефективний захист від потенційних загроз, але й сприяє створенню стійкої та надійної інфраструктури, яка відповідає сучасним вимогам безпеки в Інтернеті.

Аналіз атак із використанням вірусів вимагачів і розроблені рекомендації по протидії цим атакам можуть бути використані як звичайними користувачами, з метою збереження їхньої особистої інформації, так і представниками бізнесу і об'єктів критичної інфраструктури, для побудови надійних систем управління інформаційної безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global Cybersecurity Outlook 2022. [Електронний ресурс]. Режим доступу до ресурсу: https://www.weforum.org/reports/global-cybersecurity-outlook-2022

amed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A

tional Cybersecurity Law Review 4 (3)(2023) 259–280

лектронний ресурс]. Режим доступу до ресурсу: https://en.wikipedia.org/wiki/List_of_cyberattacks

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Valeriy Dudykevych
Doctor of Technical Sciences, Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0001-8827-9920
vdudykev@gmail.com

Oleh Harasymchuk
Ph.D., Associate Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8742-8872
oleh.harasymchuk@gmail.com

Andrii Partyka
Ph.D, Senior lecturer of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Yaroslav Sovyn
Ph.D, Associate Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

Elena Nyemkova
Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

EXPLORING THE BENEFITS OF CROSS-IMPLEMENTING CYBERSECURITY STANDARDS TO COMBAT RANSOMWARE CYBER CRIMES

Abstract. This article is devoted to research and analysis of recent cyberattacks on critical infrastructure of Ukraine using ransomware. In the article, the authors emphasize the growing importance of cyber security in today's digital environment due to the increase in the number of cybercrimes, in particular, attacks using ransomware. As a result, it is important to apply cybersecurity standards to effectively combat these threats. The article emphasizes the importance of implementing comprehensive measures that cover technical, organizational, and legal aspects to combat ransomware cybercrimes. The article also provides the main methods and tools for successfully countering ransomware, both for ordinary users and representatives of businesses and critical infrastructure facilities. Also, this paper offers an exploration of the benefits of cross-implementation of cybersecurity standards in the context of combating ransomware attacks and cybercrimes. The authors consider the methods and approaches to cyber security auditing, determine the advantages of the method of cross-implementation of standards, and offer recommendations for its effective use to ensure the security of information systems. This approach contributes to the creation of a comprehensive defense system that reduces the probability of success of attacks using ransomware and provides greater resilience of the organization to incidents and cybercrimes. The results of the study can be useful for organizations seeking to improve their cyber security and protect themselves from ransomware attacks and cybercrimes.

Keywords: information security, cybersecurity, critical infrastructure, information security management system, cybersecurity standard, cybercrime, ransomware, information systems, ISO 27001, computer networks, security monitoring, SIEM, cybersecurity audit.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Global Cybersecurity Outlook 2022. [Electronic resource]. Resource Access Mode: https://www.weforum.org/reports/global-cybersecurity-outlook-2022

amed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A

d

tional Cybersecurity Law Review 4 (3)(2023) 259–280