Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аудит інформаційної безпеки ТОВ "Се Броднетце-Україна"

Виконав(ла): студент(ка) 4 курсу, групи Сбс-42
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

		Войцьо О. М
	(підпис)	(прізвище та ініціали)
Керівник		Кареліна О. В
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Лобур Т. Б
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Загородна Н. В
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль 2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н. В
(підпис) (прізвище та ініціали)
« » 2022 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Войцю Олександру Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аудит інформаційної безпеки ТОВ "Се Борднетце-Україна"

Керівник роботи Кареліна Олена Володимирівна, к. пед. н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *23* » березня 2022 року № 4/7-178

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Технічна документація, інтернет-джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Основна частина. 1.1 Визначення аудиту інформаційної безпеки та методики його проведення. 1.2 Методики проведення аудиту інформаційної безпеки. 1.2.1 Аудит Інформаційної безпеки з метою підтвердження відповідності міжнародним стандартам. Розділ 2. Спеціальна частина. 2.1 Програми для проведення аудиту інформаційної безпеки Розділ 3. Практична частина. 3.1. Загальна інформація про філію ТОВ "Се Броднетце-Україна" 3.2 Технічна структура філії ТОВ "Се Броднетце-Україна" в Чортківському районі. 3.3 Аудит інформаційної безпеки ТОВ "Се Броднетце-Україна" Розділ 4. Безпека життєдіяльності і основи охорони праці. 4.1 Охорона праці та безпеки в надзвичайних ситуаціях.
4.2 Аналіз складових потенційної небезпеки, оцінка
рівня події та призначення безпосередньої причини події 4.3 Основні заходи щодо підвищення стійкості роботи, які здійснюються на об'єкті завчасно, за сигналами ЦЗ при раптовому Виникненні НС. Висновки. Список використаних джерел. Додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Актуальність. 3. Мета, задачі дослідження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності і основи охорони праці	Пулька Ч. В, професор кафедри МТ	25.03.2022	26.03.2022

7. Дата видачі завдання 23.03.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	23.03.2022	**Виконано**
2.	Підбір джерел про аудит інформаційної безпеки	23.03.2022	**Виконано**
3.	Опрацювання джерел про аудит інформаційної безпеки	25.03.2022	**Виконано**
4.	Підбір джерел про існуючі засоби проведення аудиту	25.03.2022	**Виконано**
5.	Опрацювання джерел про існуючі засоби проведення аудиту	28.03.2022	**Виконано**
6.	Аналіз діяльності підприємства	01.04.2022	**Виконано**
7.	Формування плану аудиту	05.04.2022	**Виконано**
8.	Вибір програмних засобів для проведення аудиту	06.04.2022	**Виконано**
9.	Оформлення розділу «Основна частина»	07.04.2022	**Виконано**
10.	Оформлення розділу «Спеціальна частина»	13.04.2022	**Виконано**
11.	Оформлення розділу «Практична частина»	17.04.2022	**Виконано**
12.	Оформлення розділу «Безпека життєдіяльності і основи охорони праці»	24.04.2022	**Виконано**
13.	Оформлення кваліфікаційної роботи	05.05.2022	**Виконано**
14.	Нормконтроль	15.06.2022	**Виконано**
15.	Перевірка на плагіат	21.06.2022	**Виконано**
16.	Захист кваліфікаційної роботи	23.06.2022	**Виконано**

Студент _____ Войцьо О. М
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кареліна О. В
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аудит інформаційної безпеки ТОВ “СЕ Борднетце-Україна” 1”// Дипломна робота освітнього рівня «Бакалавр» // Войцьо Олександр Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль 2022 // С.48 , рис. - 31, додат. – 1, бібліогр. – 10.

Ключові слова: АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПРОГРАМНІ ЗАСОБИ, КСЗІ, МІЖНАРОДНІ СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Кваліфікаційна робота присвячена проведені аудиту інформаційної безпеки, використовуючи програмне забезпечення для проведення аудиту, а також організаційні заходи. В роботі проведено аудит інформаційної безпеки та розглянуто етапи проведення аудиту інформаційної безпеки.

При проведені аудиту інформаційної безпеки було виявлено вразливості та проведено пошук вирішення проблем вирішення вразливостей в системі інформаційної безпеки (помилки програмного забезпечення, фізична безпека пристроїв, атаки ззовні) та обрано методи протидії загрозам. Доведена доцільність використання обраних програмних засобів.

ANNOTATION

Information Security Audit of SE “Bordnetze-Ukraine” 1 LLC // Thesis of educational level “Bachelor” // Voytso Oleksandr Mykolayovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBs-42 // Ternopil 2022 // P.48, fig. - 31, appendix. - 1, bibliogr. - 10.

Keywords: INFORMATION SECURITY AUDIT, SOFTWARE, KSZI, INTERNATIONAL STANDARDS OF INFORMATION SECURITY.

Qualification work is devoted to information security audits using audit software, as well as organizational activities. The paper conducted an information security audit and considered the stages of information security audit.

The information security audit identified vulnerabilities and sought to address vulnerabilities in the information security system (software bugs, physical security of devices, external attacks) and selected methods to counter threats. The expediency of using the selected software has been proved.

ЗМІСТ

ВСТУП

Аудит інформаційної безпеки проводиться з використанням програмно-апаратного забезпечення для перевірки систем інформаційної безпеки даних в організації для передачі даних їх обробки та зберігання, що в свою чергу забезпечує інформаційну безпеку під час роботи співробітників та дозволяє обробляти необхідну інформацію в межах організації.

Типи аудиту бувають: зовнішні, внутрішні, з залученням експертів, на основі міжнародних стандартів.

Існує величезна кількість програмного забезпечення, та стандартів для проведення комплексного аудиту інформаційної безпеки. Окрім програмного забезпечення для аудиту відбувається і розвиток різних апаратно-програмних засобів які потребують проведення аудиту інформаційної безпеки паралельно збільшилась і потреба їх в захисті, так як програмне забезпечення для проникнення в систему безпеки та взаємодії з ними для отримання несанкціонованого доступу до користувацьких даних стало значно більше.

Саме тому використання програмного забезпечення для проведення аудиту, представляє собою спосіб виявлення й нейтралізації вразливості за короткий проміжок часу, але і створює велику кількість вразливостей та можливостей для отримання несанкціонованих користувачів.

Система безпеки вимагає великої кількості знань та розуміння актуальності та цінності даних, що потребують захисту.

Система безпеки не може базуватися на однім методі а складається з цілого комплексу засобів захисту інформації.

Комплексна система захисту інформації – це організаційні й інженерно технічні заходи які є складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи використовуються в міру необхідності.

Тому можна стверджувати, що інформаційна безпека включає в собі захист програмного, апаратного забезпечення, персональні дані персоналу, організації.

Програмними рішеннями є спеціалізоване програмне забезпечення для захисту від вірусів, шкідливого програмного забезпечення, мережевих загроз, безпечної віддаленої роботи, контроль та обмеження доступу до мережі. Аналіз

подій пов’язаних з інформаційною безпекою. Об’єктом проведення аудиту є ТОВ «СЕ Борднетце-Україна», бізнес процеси та інформаційні потоки. Предметом проведення аудиту є принцип забезпечення захисту передачі, обробки та збереження інформації в системі, системи захисту.

Кваліфікаційна робота пояснювальної записки містить такі частини:

- у першому розділі представлені міжнародні стандарти завдяки яким можливе проведення аудиту та їх використання в процесі проведення аудиту. А також представлені порівняння того чи іншого стандарту для використання;
- у другому розділі розглянуто принцип роботи програмного забезпечення для проведення аудиту, що в свою чергу дозволяють оцінити рівень інформаційної безпеки;
- у третьому розділі проведено безпосередній аудит інформаційної безпеки організації з використанням програмних рішень, та етапи і методи нейтралізації загроз в інформаційній системі безпеки;

У висновку підсумки роботи над проведеним аудитом інформаційної безпеки, вказане програмне забезпечення, що було використано в процесі проведення аудиту.

1 ОСНОВНА ЧАСТИНА

1.1 Визначення аудиту інформаційної безпеки та методики його проведення

Аудит інформаційної безпеки – проведення об’єктивних досліджень рівня безпеки в організації. Аудит включає в собі незалежні перевірки системних файлів (логів), операцій з документами включаючи аналіз і управління системами інформаційної безпеки для виявлення прогалин технічного захисту, що виникають внаслідок неправильного конфігурування програми для технічного захисту інформації в організації. Для проведення аудиту використовуються різні методи серед них декілька видів аудиту інформаційної безпеки [1]:

- Експертний аудит – на цьому методі аудиту враховуються недоліки в системі захисту інформації з залученням досвіду експертів, що беруть участь в проведені аудиту.
- Внутрішній аудит – перевірка внутрішньої складової організації з метою оцінки механізмів організації, вивчення й оцінки контрольних перевірок у філіях, економічного розділу та інших.
- Зовнішній аудит - проводиться в самій організації, що містить в собі експертів з проведення аудиту інформаційної безпеки.
- Аудит на основі оцінки – використання цього методу передбачає проведення перевірки на відповідність певним стандартам сертифікації, стандартизації, з метою підвищення функціональних видів діяльності.

Проведення послуг аудиту несе за собою відповідальність за впровадження ключових етапів:

- Політик безпеки;
- Особистої безпеки;
- Управління і перевірка відповідності міжнародним стандартам;
- Аналіз і виявлення, перевірки оцінки вразливості для прийняття відповідних мір з мінімізації впливу або нейтралізації.

Аудит може бути проведений з використанням шаблонів або способів вивчення різноманітних принципів забезпечення інформаційної безпеки.

В цілому існують стандарти, призначенні для того щоб зовнішні і внутрішні спеціалісти могли підтримувати належну перевірку ефективності проведеного аудиту з інформаційної безпеки.

При розподілу обов’язків необхідно сформувати практичну реалізацію аудиту з використанням найкращих практик, які безпосередньо виконують процес аудиту.

Проведення аудиту з певною періодичністю необхідне для забезпечення захисту даних на належному рівні. Крім того необхідно підтвердити такі дії як:

- зміну конфігураційних файлів;
- встановлення новітнього програмного забезпечення або його оновлення;
- закупка нового апаратного та програмного забезпечення які потребують належного аудиту після їх експлуатації;

Аудит включає в собі формування навичок з використанням інформаційних технологій. Крім того аудитор безпосередньо взаємодіє з системою безпеки щоб забезпечити належний захист, для цього отримують сертифікати які відповідаю за певний вид захисту на основі інформаційних технологій:

- Менеджер з Інформаційних систем (CISM);
- Управління інформаційними системами на основі управління ризиками (CRISC);
- Управління в області корпоративного IT (CGEIT);
- Аудитор інформаційних систем (CISA);
- Основні навички з інформаційної безпеки Nexus (CSX);
- Спеціаліст з кібербезпеки Nexus (CSXP).

Отже аудит потребує комплексного підходу, і зазвичай не завжди всі міри захисту допомагають, навіть перешкоджають нормальній роботі оскільки більше часу піде на проходження систем безпеки. В свою чергу це створить незручності для працівників які тільки розпочинають свою кар’єру.

1.2 Методики проведення аудиту

Найпоширенішими методиками проведення аудиту є зовнішні, внутрішні, на основі експертної оцінки, згідно міжнародних стандартів. Зовнішній аудит

проводиться на основі залучення сторонньої організації яка безпосередньо проводить аудит. Внутрішній аудит проводиться безпосередньо в організації яка містить підрозділ безпеки [2].

Аудит на основі експертної оцінки проводиться з залученням експертів які оцінюють актуальність стану інформаційної безпеки підприємства. Використання міжнародних стандартів дозволяє оцінити актуальність організації яка дотримується спеціальних стандартів які формують інформаційну безпеку підприємства. Виконавцями аудиту можуть бути:

- Державний орган – в першу чергу вони проходять підготовку щоб отримувати можливість проводити аудит інформаційної безпеки і стати потенційним партнером для регулювання усіх питань аудиту.
- Корпоративні внутрішні аудитори – безпосереднього проводиться під керівниками організації, його можуть проводити тільки аудитори яких замовила або сформувала організація.
- Зовнішні аудитори – зазвичай це стороння організація яка має навички проведення аудитів інформаційної безпеки і здатна проводити вузькоспеціалізовані аудити.
- Спеціаліст з інформаційної безпеки – завдяки такій організації відбувається моніторинг систем безпеки і підтримує баланс ризиків для організації.

Основними цілями які займаються аудитори інформаційної безпеки складають:

- Формують експертну оцінку – тобто формування політик і стандартів безпеки з встановленням особистої безпеки організації яка в свою чергу використовуватиме свої активи для функціонування підприємства з можливістю контролю доступу у відповідність обслуговування і реагування. Виявлення технічних негараздів і миттєвої нейтралізації.
- Підготовка і планування – виконати даний пункт аудитор зможе лише покладаючись на інформацію яку отримав з експертної оцінки. Завдяки такій оцінці можливо сформувати план і докази для перевірки лише окремих ланок організації. Це в свою чергу дозволяє спрогнозувати на, що підуть гроші щоб вирішити те чи інше питання не вводячи постійних перевірок.

- Ціль аудиту – формується лише тоді коли проаналізовані всі можливі фактори або ризики які якимось чином впливатимуть на підвищення виникнення ризиків.
- Виконання аудиту – відбувається збір усіх можливих даних для виявлення потенційних порушників. Воно включає в собі перевірку з чітко сформованих цілей аудиту.
- Написання аудиторського висновку – після завершення усіх процедур аудиту формується відповідний документ з усіма можливими правками, покращеннями, рекомендаціями для представлення її для організації з метою зацікавити організацію в формуванні політик інформаційної безпеки та захисту інформації в організації.
- Формування кінцевого висновку – кінцевий висновок повинен бути суміжним з створеним аудиторським висновком, у ньому формуються усі запити які були враховані і підлягають поясненню, що ця перевірка собою являє.

Вся ця інформація не повинна попадати в санкціонований доступ. Як правило висновок в загальному показує рекомендації які необхідно виконати для покращення системи захисту інформації в організації.

1.2.1 Аудит інформаційної безпеки з метою підтвердження відповідності міжнародним стандартам.

Кожен стандарт відповідності має власні вимоги, але багато правил перетинаються. Наприклад, HIPAA захищає медичні дані, а PCI-DSS захищає фінансові дані, але обидва мають схожі вимоги до шифрування даних, зберігання конфіденційної інформації та контролю доступу до авторизації. Першим кроком у відповідності є пошук стандартів, релевантних для бізнесу.

Для найефективнішого проектування інфраструктуру спочатку слід будувати з урахуванням відповідності, але старі підприємства можуть мати існуючу інфраструктуру, яка була побудована десятиліття тому. Стандарти відповідності постійно переглядаються та оновлюються, тому будь-які нові правила повинні бути визначені та проаналізовані. Якщо організація не впровадить нові правила

відповідності до своєї поточної інфраструктури, вона може порушити її та загрожує значним штрафам.

Більшість стандартів належать до наступних категорій контрольного списку відповідності IT [3]:

- Контроль доступу та ідентифікації - Цей стандарт визначає правила аутентифікації та авторизації.
- Контроль над обміном даними. Організація повинна мати суворий контроль за даними, якими передається громадськістю і клієнтами.
- Реакція на інцидент. Це положення керує організацією щодо пом'якшення, звітування та розслідування порушень даних.
- Аварійного відновлення. Коли інфраструктура виходить з ладу, організації повинні відновити резервні копії та продуктивність. Стандарти аварійного відновлення скорочують тривалість простоїв, щоб не постраждали продуктивність і прибуток.
- Запобігання втрати даних. Щоб уникнути втрати даних, у відповідності визначено, що робити, щоб захистити прибуток і продуктивність бізнесу, включаючи резервне копіювання, відновлення та резервування.
- Захист від шкідливих програм. Антивірусні та інші засоби захисту від шкідливого програмного забезпечення захищають інфраструктуру від шкідливого коду, і кожен стандарт вимагає цього у всьому середовищі, включаючи сервери та пристрої користувачів.
- Корпоративна політика безпеки. Організація повинна розробити політики, яких користувачі повинні дотримуватися для захисту даних.
- Моніторинг та звітність. Без моніторингу організація вразлива до постійних загроз. Звітування дає адміністраторам можливість переглядати справність своїх систем.

Організації зобов'язані створювати системи, які захищають конфіденційність і безпеку даних клієнтів. Існує кілька ключових причин, чому ці стандарти відповідності IT-безпеці існують і ретельно контролюються.

Положення розроблені, щоб допомогти компаніям покращити свої стратегії інформаційної безпеки, надаючи найкращі методи та рекомендації на основі їх галузі та типу даних, якими вони керують і зберігають.

Недотримання цих стандартів може призвести до таких наслідків, як порушення даних. Інші ключові переваги стандартів відповідності IT-безпеці включають:

- Підвищений контроль над безпекою бізнесу, що призводить до зменшення кількості помилок і зменшення внутрішніх і зовнішніх загроз;
- Менше фінансових втрат через порушення даних і пов'язані з цим витрати, такі як витрати на ремонт і юридичні витрати;
- Покращені заходи безпеки, дотримуючись найкращих методів та вказівок щодо відповідності вимогам безпеки IT;
- Збереження довіри до клієнтів, оскільки споживачі, швидше за все, довірятимуть компанії, якщо знають, що їхня інформація безпечна.

Зараз існує багато стандартів безпеки інформаційних технологій США. Деякі з найпоширеніших включають:

- GDPR (The General Data Protection Regulation) - це закон про безпеку та конфіденційність, створений Європейським Союзом. Стандарт розроблений для захисту громадян ЄС від порушення даних і застосовується до всіх компаній, які обробляють персональні дані людей, які проживають в ЄС, включаючи компанії, які фізично не розташовані в Європейському Союзі.

- HIPAA - Закон про перенесення та підзвітність медичного страхування був прийнятий у 1996 році Конгресом і є федеральним законом. HIPAA включає серію стандартів для даних про медичне обслуговування в електронних рахунках. Він також дозволяє передавати та продовжувати медичне страхування для американських працівників та їхніх сімей, коли вони втрачають або змінюють роботу.

- PCI DSS (The Payment Card Industry Data Security Standard) - це широко відомий стандарт безпеки, розроблений для того, щоб допомогти підприємствам активно захищати дані облікових записів клієнтів. Цей стандарт створений у 2004 році компаніями MasterCard, Visa, American Express, JCB International та Discover Financial Services і допомагає захистити транзакції з дебетовими та кредитними картками від шахрайства та крадіжки.

- NIST (The National Institute of Standards and Technology) - є важливим ресурсом для технологічної безпеки та розвитку багатьох підприємств по всій країні. Дотримання стандартів NIST є важливим пріоритетом майже в усіх галузях, які

мають справу з технологіями. Стандарти NIST засновані на передовому досвіді організацій безпеки, публікаціях і документах.

- FISMA (The Federal Information Security Management Act) - створений у 2002 році і зобов'язує федеральні агентства розробляти та впроваджувати програми безпеки та захисту даних. Стандарт введено, щоб допомогти зменшити ризики безпеки даних, одночасно керуючи витратами на безпеку даних.

- CIS Controls (The Center for Internet Security) - це широко прийнята група заходів для інформаційної безпеки. Ці стандарти були введені, щоб запобігти небезпечним кібератакам та іншим внутрішнім і зовнішнім загрозам . Основною метою Контролю є захист важливої інфраструктури, активів та інформації.

Найочевидніший і найбезпечніший спосіб з'ясувати, які аудити вам потрібно пройти – це проконсультуватися з юристами та працівниками служби інформаційної безпеки. Зазвичай відповідність IT зосереджується на трьох типах даних [4]:

- Особиста інформація - будь-яка інформація, що стосується особи, яку можна ідентифікувати: ім'я, домашня адреса, дата та місце народження, біометричні записи;
- Захищена інформація про здоров'я - результати медичних оглядів, інформація про плани охорони здоров'я, будь-які медичні записи, які можна пов'язати з конкретною особою;
- Фінансові дані - номери кредитних карток, дані про доходи та витрати, фінансові звіти фізичної особи, організації чи будь-якої іншої особи;

Після того, яких стандартів, законів і правил потрібно дотримуватися, ви можете призначити персонал, відповідальний за дотримання цих стандартів. І GDPR, і PCI DSS вимагають, щоб організація призначала співробітника, який відповідає за дотримання. Але якщо вам потрібно дотримуватися інших стандартів, законів і правил, призначення DPO все одно приносить кілька переваг [5]:

- Експертне знання законодавства про інформаційну безпеку. Відповідно до GDPR, DPO має підтвердити свій досвід у захисті даних та знання відповідних законів, правил і стандартів.
- Постійний моніторинг стану відповідності IT. У той час як інші співробітники зосереджуються на своїх обов'язках між аудитами, DPO

відстежує зміни вимог, зміни в системі інформаційної безпеки організації та відповідність поточних засобів контролю безпеки поточним вимогам захисту інформації.

- Чітке та швидке повідомлення про порушення . У разі порушення безпеки DPO має організувати групу реагування на інциденти, повідомити всіх, хто постраждав від порушення, та повідомити про це владі та клієнтам. Швидка реакція на порушення безпеки пом’якшує його наслідки та зменшує суму штрафів.

Яким корисним не був DPO, важливо пам’ятати, що одна особа не може забезпечити відповідність організації, щоб покращити існуючі засоби контролю та політики безпеки, виконати налаштування існуючого програмного забезпечення та розгорнути нове програмне забезпечення. Для цього необхідно провести оцінку ризиків з якими може зіткнутися організація:

- ризики та загрози інформаційної безпеки для вашої організації;
- активи, які є критичними для вашої організації та підпадають під дію нормативно-правових актів;
- поточний рівень захисту, а також слабкі та сильні сторони вашого захисту.

Результати оцінки ризиків будуть корисні для планування покращень безпеки, а також для розробки нових політик і стратегій. Після розробки нових політик і стратегій необхідно провести самостійний аудит.

Самостійний аудит має багато спільного з оцінкою ризику: це оцінка запроваджених засобів контролю безпеки. Але на відміну від оцінки ризиків, самостійний аудит допомагає вам оцінити ваш поточний рівень відповідності та виявити прогалини в захисті даних. Це також готує ваших співробітників до справжнього IT-аудиту.

Щоб провести самостійний аудит і відповідав усім вимогам аудиту, необхідно слідкувати і дотримуватися усіх інструкцій аудиту з відповідності інформаційної безпеки:

- Оцінка ресурсів та аудиту за стандартом NIST;
- Відповідність контрольного списку за стандартом GDPR;
- Відповідність контрольного списку за стандартом HIPPA.

Єдиним великим недоліком самостійного аудиту є їх досить висока вартість, як з точки зору грошей, так і часу. В результаті оцінки ризиків та самостійного аудиту сформується список політик, практик і технічних засобів контролю, які потрібно застосувати, щоб пройти аудит інформаційної безпеки.

Щоб спростити та прискорити реалізацію необхідних засобів контролю, найкраще створити журнал аудиту IT. Журнал аудиту IT - це набір записів, які описують будь-які дії з конфіденційними даними, базами даних, програмами або частинами вашої інфраструктури.

Це дозволяє перевірити відповідності вимогам інформаційної безпеки, як ваші співробітники обробляють чутливі ресурси, і є важливою частиною будь-якого аудиту відповідності та безпеки.

Реєстрація аудиторського сліду також корисна для моніторингу безпеки та розслідування інцидентів. Використовуючи згенеровані журнали, необхідно відстежувати будь-які дії у захищеному середовищі, виявляти інциденти безпеки та оцінювати джерела загроз.

Він повинен реєструвати всі дії користувача, зберігати їх у захищеному форматі та надавати докази зловмисної активності. Записи моніторингу також корисні під час судово-медичної діяльності та розслідування.

Аудит відповідності проводиться регулярно, а це означає, що вам потрібно постійно переглядати та покращувати свої заходи безпеки, щоб залишатися відповідними. Ось чому вам потрібно створити стратегію відповідності - набір внутрішніх політик і процедур, які допоможуть вашій організації залишатися відповідним.

Після того, як стратегія відповідності буде завершена, важливо призначити людей, відповідальних за її виконання. Зазвичай за цю стратегію відповідає уповноважений із захисту даних або головний спеціаліст із захисту інформації.

Деякі дії під час аудиту відповідності доводиться виконувати вручну: перегляд політик, розслідування інцидентів із безпекою, співпраця з органом із сертифікації тощо.

Проте автоматизовані інструменти допомагають зменшити витрати на відповідність, заощадити час на підготовку до аудиту та мінімізувати ризик людських помилок.

За допомогою спеціального рішення щодо відповідності автоматизувати:

- постійний моніторинг безпеки;
- впровадження політики управління доступом;
- сповіщення про підозрілі дії;
- збір даних для аудиту;
- звітність.

Для проходження аудиту всі співробітники, які працюють з конфіденційними даними, повинні розуміти свої обов’язки та використовувати безпечні методи. Іноді це означає, що їм доводиться скорегувати або змінити свої робочі процеси.

Щоб допомогти співробітникам зрозуміти свою роль у процесі аудиту, необхідно:

- пояснити, як витік даних і невдалий аудит вплинуть на організацію;
- ділитися інформацією про порушення безпеки у вашій галузі;
- проводити тренінги з інформаційної безпеки;
- розповісти про важливість нових засобів контролю безпеки;
- описати результат невідповідності.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Програми для проведення аудиту інформаційної безпеки

Після ухвалення всіх можливих рішень відбувається безпосередній аудит безпеки інформаційних систем з використанням програм які сканують найбільш поширені вразливості в системі, серед них:

- Burp Suite - модульний сканер для виконання тестування безпеки веб-додатків.
- OpenVAS - повнофункціональний сканер вразливостей з можливістю тестування.
- Nmap – сканер для проведення розвідки та аудиту безпеки мережі.
- Nessus – сканер вразливостей який визначає рівень захисту інформаційної безпеки на основі конфігурацій адміністратора інформаційної безпеки з виявленням поширених вразливостей.

Burp Suite є найпопулярнішим інструментом, який використовується для оцінки безпеки веб-додатків. Цей інструмент доступний як Burp Suite Community Edition, Burp Suite Professional і Burp Suite Enterprise Edition. Основні інструменти які доступні з використанням Burp Suite:

- Spider – завдяки йому отримуються кінцеві точки, щоб спостерігати за їх функціональністю та знаходити потенційні вразливості. Основна мета використання цього модуля – знаходити кінцеві точки для виявлення вразливостей і нейтралізації під час проведення розвідки або тестування на виявлення потенційних вразливостей (див. рис.2.2.1):

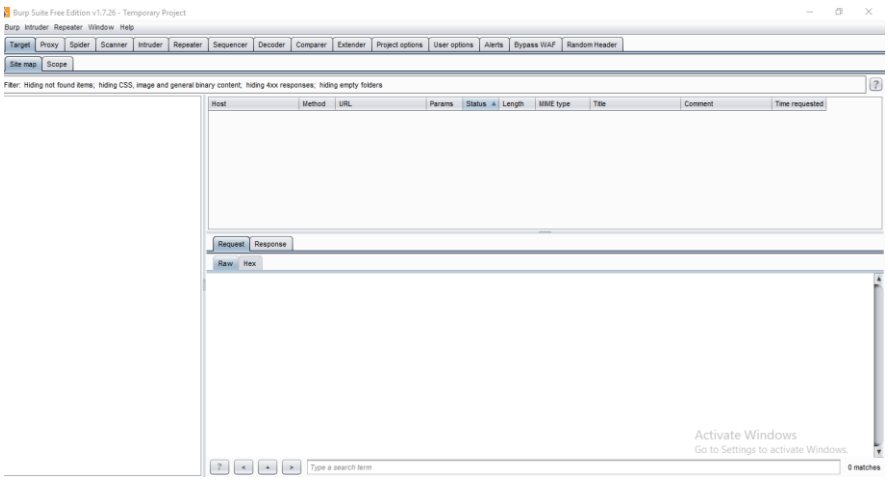

Рисунок 2.2.1 – Головне вікно модуля Spider

- Proxy – дозволяє бачити і змінювати вміст відповідей під час їх передачі. Проксі-сервер можна налаштувати так, щоб він працював на певному зворотному IP-адресі та порту. Проксі-сервер також можна налаштувати для фільтрації певних типів пар запит-відповідь (див.рис.2.2.2):

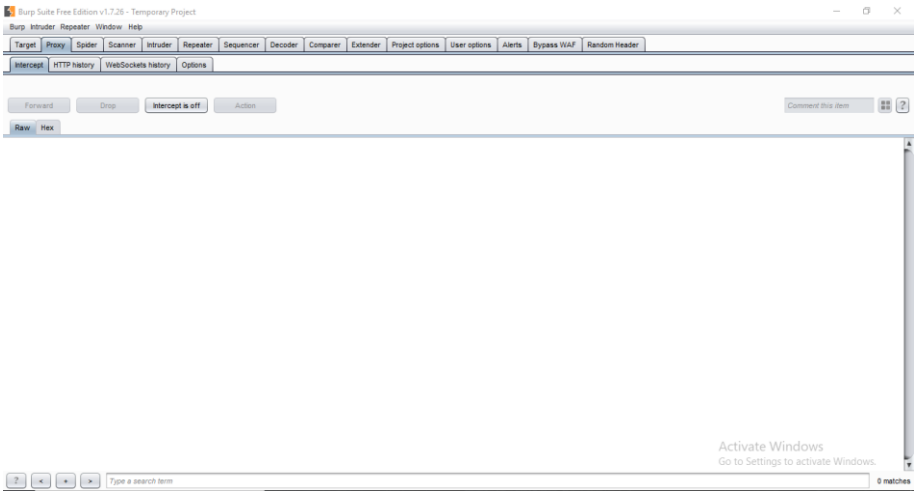

Рисунок **2.2.2 –** Головне вікно модуля Proxy

- Intruder – використовується для проведення перевірки на xss-атаки, sql-ін’єкцій, bruteforce-атак, підміни паролів в формах (див.рис.2.2.3):

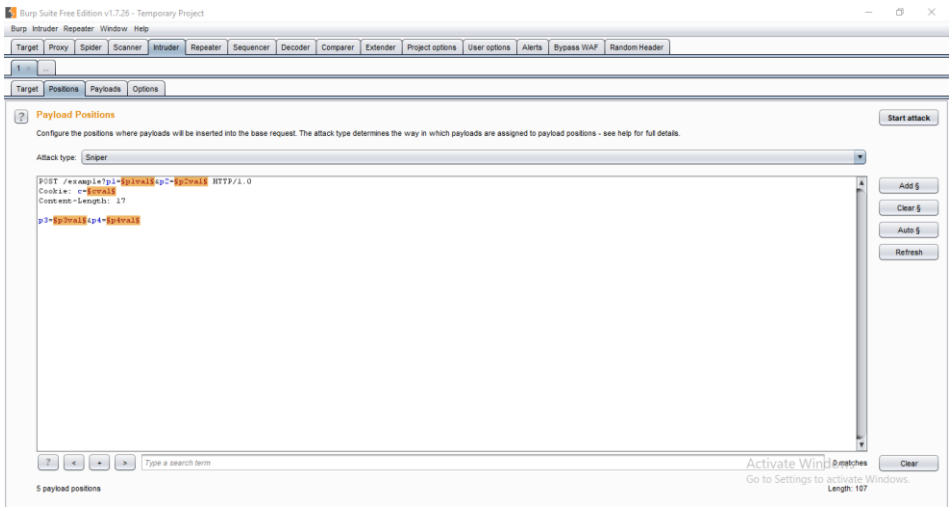

Рисунок 2.2.3 – Головне вікно модуля Intruder

- Repeater – використовується для перевірки введених значень, оцінки виконання, параметрів запиту, перевірка очищення даних сервером, виявлення несподіваних значень і помилок під час передачі даних, перевірка реалізацій захисту CSRF з можливістю повторного надсилання запитів з внесенням змін вручну (див.рис.2.2.4):

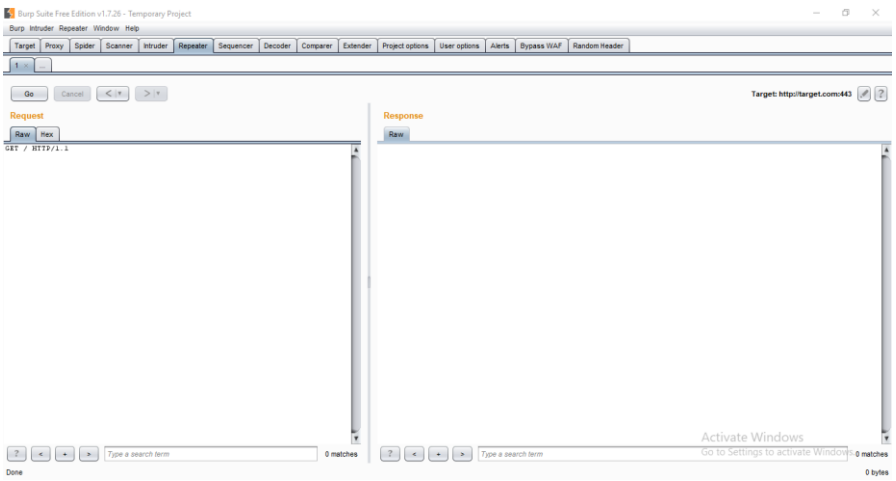

Рисунок 2.2.4 – Головне вікно модуля Repeater

- Sequencer – засіб для перевірки ентропії який перевіряє випадковість маркерів згенерованих веб-сервером. Ці маркери використовуються для аутентифікації в конфіденційних операціях: прикладами таких маркерів є файли cookie та маркери анти-CSRF (див.рис.2.2.5):

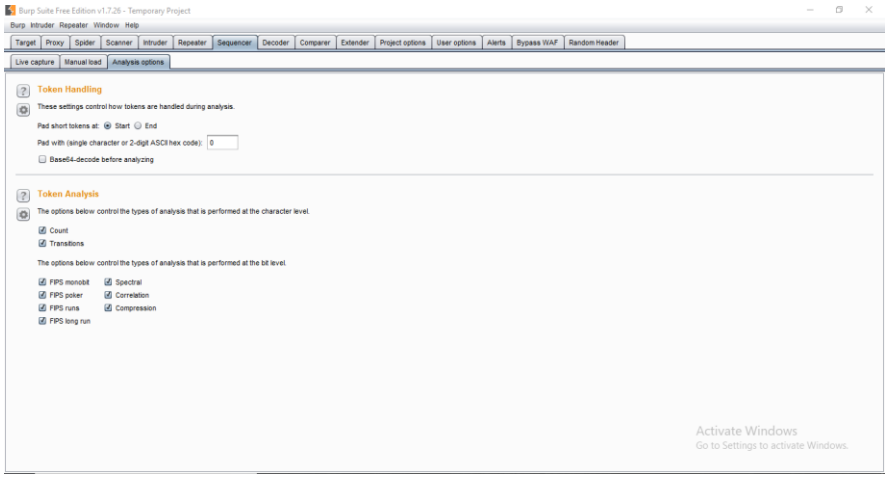

Рисунок 2.2.5 – Головне вікно Sequencer

- Decoder - містить список поширених методів кодування, таких як URL, HTML, Base64, Hex тощо. Цей інструмент зручний під час пошуку фрагментів даних у значеннях параметрів або заголовків. Він також використовується для створення корисного навантаження для різних класів уразливості (див.рис.2.2.6):

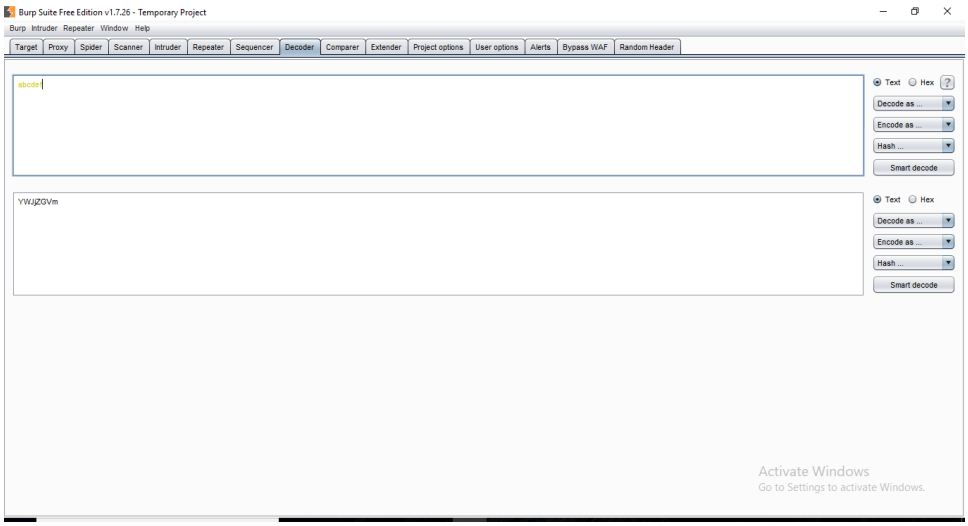

Рисунок 2.2.6 – Головне вікно Decoder

- Extender – модулі завдяки яким розширюються можливості як використання Burp Suite, проведення аудитів, тестів, різноманітних компонентів системи безпеки (див.рис.2.2.7):

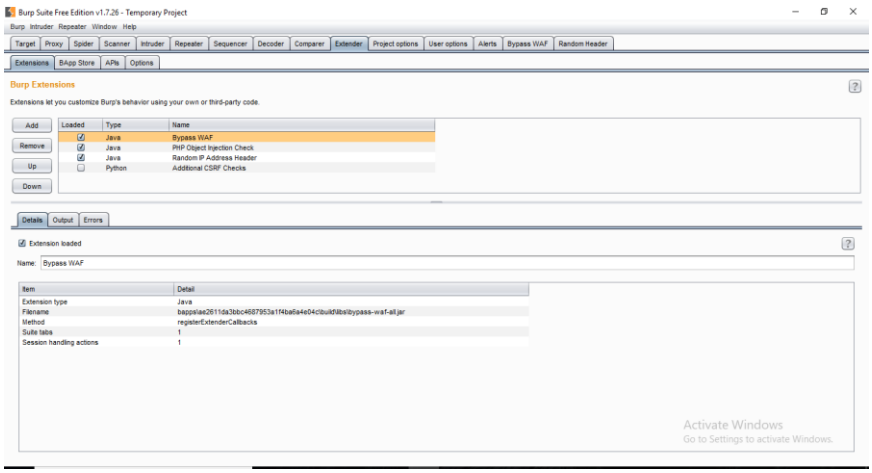

Рисунок 2.2.7 – Головне вікно Extender

- Scanner – автоматично сканує веб-сайти на наявність багатьох поширених вразливостей і перераховує їх з інформацією про достовірність кожної помилки та складності їх використання. Але Scanner недоступний на версії Community Edition.

nmap – інструмент який використовується для сканування IP-адрес запущені в їхній мережі, виявляти відкриті порти та служби, а також виявляти вразливості. Основні функції nmap включають:

- Допомагає визначити служби, запущені в мережі;
- nmap може знайти інформацію про операційну систему, запущену на пристроях.
- Збирати статистичну інформацію про мережевий трафік.

Nmap також пропонує гнучку специфікацію цілі та порту, сканування, сканування sunRPC . Більшість платформ Unix і Windows є такими підтримується як в режимах GUI, так і в режимах командного рядка (див.рис.2.2.8):

```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$
```

Рисунок 2.2.8 – Інтерфейс командного рядка nmap

OpenVAS - це повнофункціональний сканер вразливостей, завдяки якому виявляються застарілі мережеві служби, відсутні виправлення безпеки, погано налаштовані сервери та інші вразливості. Він також інтегрується з багатьма іншими популярними платформами безпеки, такими як OSSEC і Snort. Особливості полягають в наступному:

- Підтримує сканування вразливостей 26 000 CVE;
- Доступний веб-інтерфейс;
- Експортує звіти про вразливості у форматі HTML, PDF, CSV;

Nessus – інструмент для перевірки вразливостей які могли б використовувати хакери з метою отримання конфіденційної інформації.

Nessus працює, перевіряючи кожен порт на комп'ютері, визначаючи, яка служба на ньому запущена, а потім перевіряючи цю службу, щоб переконатися, що в ній немає вразливостей, які можуть бути використані хакером для здійснення зловмисної атаки. До особливостей програми можна віднести:

- Сканування вразливостей, які можуть дозволити несанкціонований контроль або доступ до конфіденційних даних у системі;
- Виявлення неправильних конфігурацій системи безпеки.
- Сканування тимчасових кінцевих точок, які не завжди підключені до локальної мережі.
- Підвищення загальної продуктивності сканування: за допомогою агентів сканування мережі можна звести лише до віддаленої перевірки мережі, що прискорює час завершення сканування.

Nessus виконує сканування за допомогою плагінів, які запускаються на кожному хості в мережі, щоб виявити вразливі місця.

Після виконання всіх кроків Nessus запускає кожен хост із базою даних відомих уразливостей, намагаючись виявити, який хост містить які вразливості. Nessus дає вам можливість налаштувати сканування на основі різних шаблонів сканування та політики. Ці шаблони визначать параметри, які будуть знайдені в налаштуваннях політики сканування.

3 ПРАКТИЧНА ЧАСТИНА

3.1 Загальна інформація про філію ТОВ “СЕ Борднетце-Україна”

Компанія SEBN утворилася в результаті придбання компанією Sumitomo Electric Industries компанії Volkswagen Bordnetze GmbH і ця історія маю дві гілки історії:

- Sumitomo – заснований 1897 року. Сьогодні є одним з інтернаціональних постачальників автопродукції.

- Bordnetze – створена в 1986 році двома провідними німецькими компаніями Volkswagen AG і Siemens AG і була названа Volkswagen Bordnetze GmbH.

У 2006 році утворилася компанія Sumitomo Electric Bordnetze (SEBN). Компанія виготовляє кабельно-провідникову продукцію для автомобілів, а саме - електричне з’єднання компонентів в автомобілі, як наприклад, приладів управління, фар, покажчиків поворотів, реле і т.д. Виготовляється кабельно-провідникова продукція для автомобілів марки:

- AUDI E-Tron;
- AUDI C8 (A7/A6);
- Volkswagen Golf A8;
- PORSCHE J1.

Сам кабель візуально розглядається як «електричні жили» транспортного засобу. Без цих функцій системи безпеки, такі як ABS, ESP, або зручні для користувача функції, як-от підігрів сидінь, електричний склопідйомник або блок клімат-контролю, не працюватимуть. Філія SEBN-UA знаходиться в таких містах України (див.рис.3.1.1):

- Тернопіль;
- Чортків ;
- Чернівці.

Рисунок 3.1.1 – Розташування філій SEBN в Україні

Для забезпечення мережевого з'єднання між всіма філіями, що розміщені в Україні використовується мережевий кабель для підключення роутерів і взаємодія з ними в радіусі 50 км. (див.рис. 1.6):

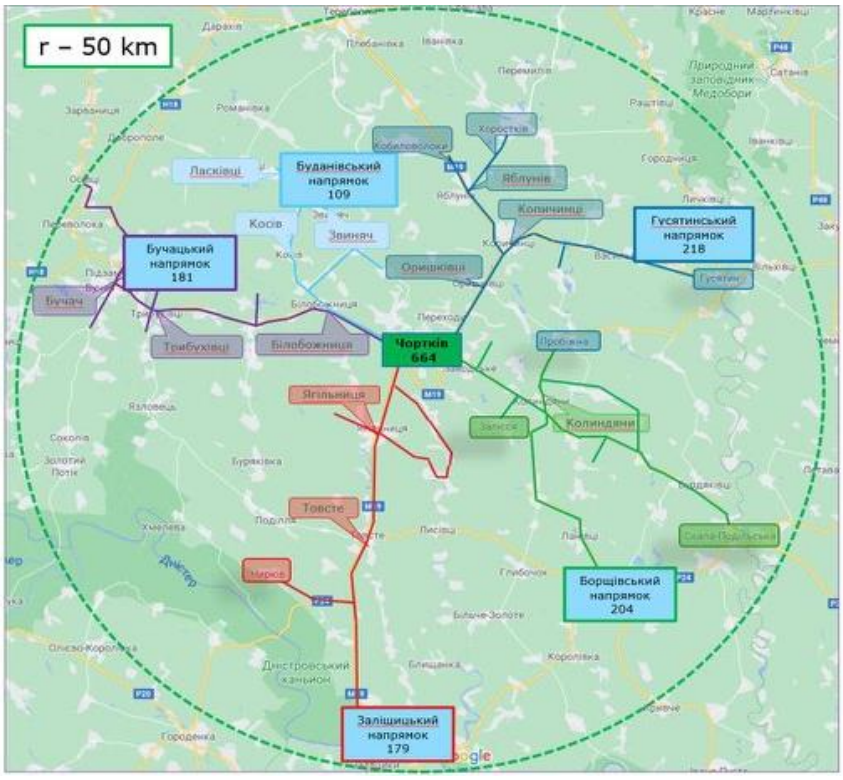

Рисунок 3.1.2 - Кабельно мережеве з'єднання філій SEBN-UA в місті Тернопіль, Україна.

Філії SEBN розташовані в більшості країнах Європи, Азії, США і інших країн (див.ри.3.1.3):

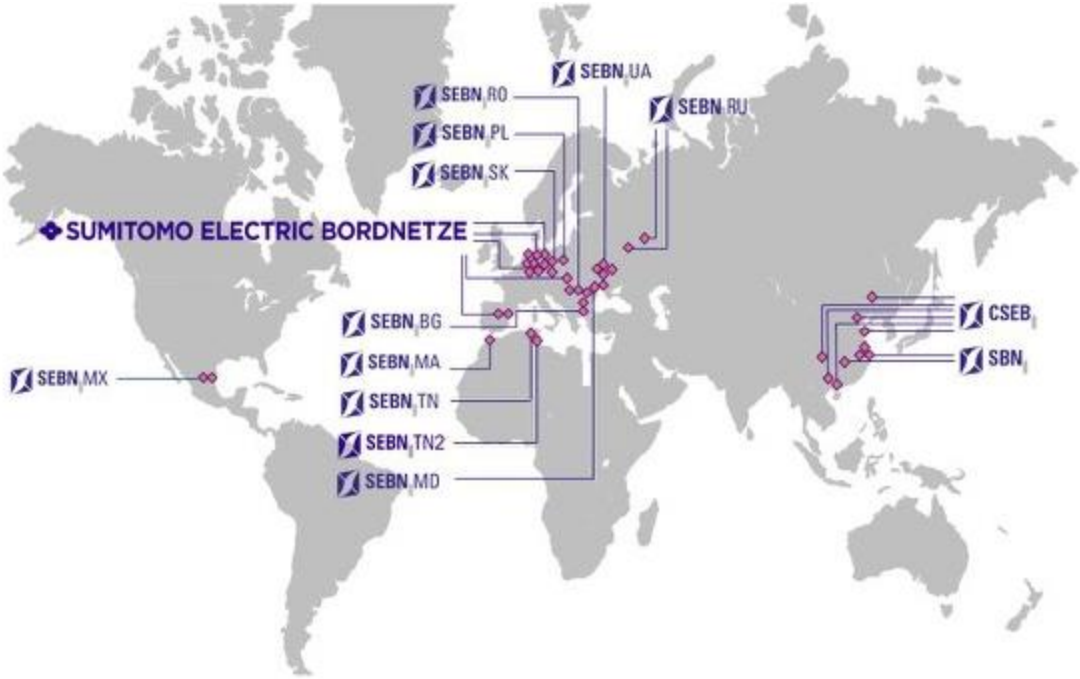

Рисунок 3.1.3 – Розташування філій SEBN по всьому світу

3.2 Технічна структура філії ТОВ “СЕ Борднетце-Україна” в Чортківському районі.

Для забезпечення безпечної, продуктивної умови праці використовується пропускна система завдяки якій проводиться полегшення ведення обліку працівників на підприємстів, щоб уникнути надзвичайних ситуацій під час роботи в виробництві допускаючи працівників які працюють в SEBN-UA.

Використання системи ідентифікації дозволяє автоматизувати процес роботи працівника на робочому місці, замовлень та отримання обідів у їдальні, отримання даних працівником на інформаційних моніторах з метою ведення обліку робочого часу працівника.

Характеристики ІКС Чортківської філії ТОВ «СЕ Борднетце-Україна» складається з такого виду обладнання:

Персональні комп’ютери Dell OptiPlex 3050 Micro в кількості – 260 шт. На них використовується операційна система Microsoft Windows LTSC версії Windows 10 1809 (2019) (див.рис.3.2.1):

Рисунок 3.2.1 - Загальний вигляд ПК Dell OptiPlex 3050 Micro

Всі комп’ютери підключені до моніторів Dell: E1920H (див.рис.3.2.2):

Рисунок 3.2.2 - Монітор Dell: E1920H

Для «Попереднього виробництва» використовуються такі засоби як (див.рис.3.2.3):

Рисунок 3.2.3 - Стенд для монтажу і закручування кабелів для автомобілів

Додаткові пристрої та матеріали які містяться в стендах:

- Зварювальних апаратів в кількості - 21 шт.
- Охолоджувальних машин в кількості - 16 шт.
- Скручувальних машин в кількості - 24 шт.

Для виготовлення кабельно-провідникової продукції автомобіля марки AUDI E-Tron використовуються:

- Формуючі дошки в кількості - 45 шт.
- Конвеєрних ліній в кількості - 9 шт.
- Тестових таблиць в кількості -15 шт.
- Позиції в кількості - 1 шт.

Для виготовлення кабельно-провідникової продукції автомобіля марки AUDI C8 (A7/A6) використовуються:

- Формуючі дошки в кількості - 90 шт.
- Конвеєрних ліній в кількості - 3 шт.
- Тестових таблиць в кількості - 18 шт.
- Системи відеонагляду в кількості - 2 шт.

Для виготовлення кабельно-провідникової продукції автомобіля марки Volkswagen Golf A8 використовуються:

- Формуючі дошки в кількості - 55 шт.
- Тестових таблиць в кількості - 24 шт.
- Конвеєрних ліній в кількості - 29 шт.
- Системи відеонагляду в кількості – 3 шт.

Для виготовлення кабельно-провідникової продукції автомобіля марки PORSCHE J1 використовуються:

- Формуючі дошки в кількості - 55 шт.
- Формуючі дошки класу GSTARS в кількості - 4 шт.
- Конвеєрних ліній в кількості - 17 шт.
- Тестових таблиць в кількості – 15 шт.
- Позиції в кількості – 3 шт.

Філія SEBN-UA використовує операційну систему Microsoft Windows Server 2012 R2 з сконфігурованою системою яка називається Active Directory.

3.3 Аудит інформаційної безпеки ТОВ “СЕ Борднетце-Україна”

Для того щоб зрозуміти як розпочати аудит необхідно зрозуміти якими активами або програмним забезпеченням користується організація для цього використовуємо такі інструменти як:

- DNS Dumpster;
- Shodan;

DNSDumpster - це інструмент для пасивного збору інформації. Інструмент DNSDumpster є найкориснішим інструментом для розвідки DNS, виконання записів MX, TXT, пошуку NS, перерахування субдоменів тощо [6].

DNSDumpster буде збирати інформацію з доступних ресурсів з відкритим кодом і надавати нам дані пасивно . Натомість DNSDumpster не буде переборювати субдомени для перерахування субдоменів, він запитуватиме ресурси з відкритим кодом і збирати звідти дані.

Shodan - це база даних з мільярдів загальнодоступних IP-адрес, яку експерти з безпеки використовують для аналізу безпеки мережі [2].

Shodan працює, запитуючи з'єднання з усіма можливими адресами Інтернет-протоколу (IP) в Інтернеті та індексуючи інформацію, яку він отримує від цих запитів на підключення. Shodan сканує в Інтернеті пристрої за допомогою глобальної мережі комп'ютерів і серверів, які працюють цілодобово. Однак Shodan показує, яка частина нашої інформації є загальнодоступною.

Перейдемо до використання інструментів для знаходження активів ТОВ "СЕ Борднетце-Україна". Для використання DNS Dumster необідно перейти за посиланням https://dnsdumpster.com. Після того ввести домен веб-сайту яким необхідно проаналізувати (див.рис.3.3.1):

Рисунок 3.3.1 – Результати виведення інструменту DNS Dumster в домені sebn.com

В результаті аналізу відображаються наступні дані – Карта доменних імен sebn.com (див.рис.3.3.2):

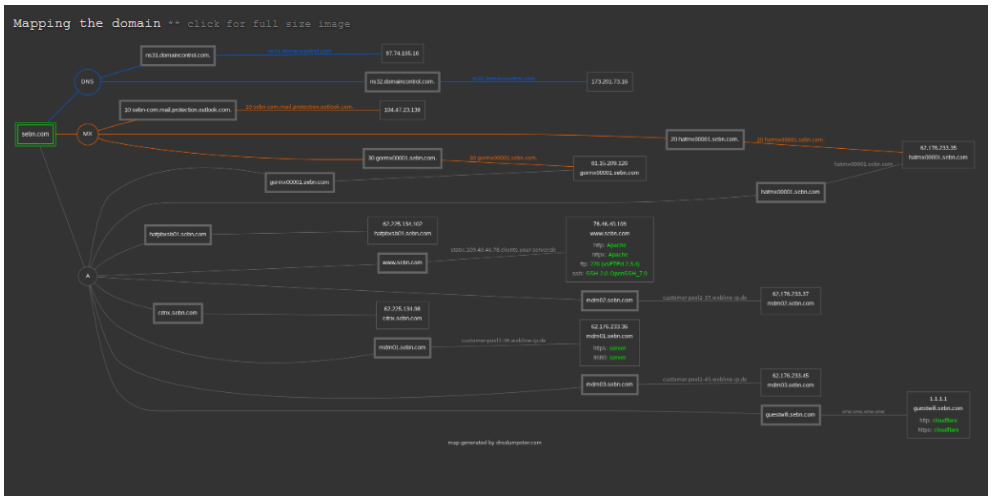

Рисунок 3.3.2 - Карта доменних імен sebn.com

Розміщення і адреси DNS серверів sebn.com (див.рис.3.3.3):

DNS Servers

ns31.domaincontrol.com.	97.74.105.16 ns31.domaincontrol.com	GODADDY-DNS United States
ns32.domaincontrol.com.	173.201.73.16 ns32.domaincontrol.com	GODADDY-DNS United States

MX Records ** This is where email for the domain goes...

10 sebn-com.mail.protection.outlook.com.	104.47.23.138 mail-tycjpn010138.inbound.protection.outlook.com	MICROSOFT-CORP-MSN-AS-BLOCK Japan
30 gormx00001.sebn.com.	81.15.209.126 gormx00001.sebn.com	ASN-TELENERGO ul. PERKUNA 47, WARSZAWA Poland
20 hatmx00001.sebn.com.	62.176.233.35 hatmx00001.sebn.com	WOBCOM Germany

Рисунок 3.3.3 – Адреси DNS серверів та розміщення їх в різних країнах

Дані з певного текстового файлу який витягнув інструмент DNS Dumpster (див.рис.3.3.4):

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"MS=ms61244608"
"amazonses:oqTMxRUV8Y44l6OcWiNQIIPmYMBIFJtQTJ1HF9v/UyI="
"v=spf1 mx ip4:197.230.133.147 ip4:188.64.192.50 ip4:143.164.102.17 ip4:18.196.215.67 ip4:62.225.134.98 ip4:194.114.62.75 ip4:5.58.242.151 ip4:82.207.83.6 ip4:5.58.242.152 ip4:82.207.83.5 ip4:189.204.198.26 ip4:41.205.194.179 ip4:196.179.224.250 ip4:86.34." "190.141 ip4:195.146.149.94 ip4:195.22.240.42 ip4:83.228.75.226 include:recruitmail.com include:spf.protection.outlook.com -all"
"MS=ms95787004"
"apple-domain-verification=NnWS3wuoD4k7AdPG"
"google-site-verification=oByAXqS8NIWh743fWEkQ3KXqzcM4X2rRkDJNJaYOoN4"
"v=verifydomain MS=2852256"

Рисунок 3.3.4 – Конфіденційні дані з текстового файлу

Детальніше про конфіденційні дані можете розглянути в – Додатку А. Переходимо до інструменту Shodan. Даний інструмент надає необхідну можливу відкриту інформацію для цього я введу домен sebn.com (див.рис.3.3.5):

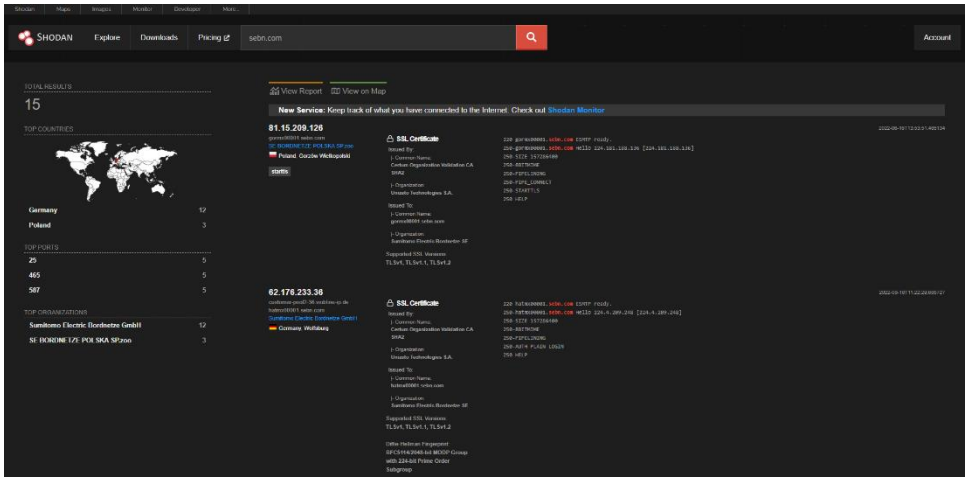

Рисунок 3.3.5 – Список IP-адрес які використовує філія SEBN

Оскільки дізналися за допомогою інструментів Shodan і DNS Dumpster необхідні точки для проведення аудиту – необхідно провести аналіз вразливостей. Для цього використаємо інструменти:

- Nessus;
- OWASP ZAP;

Nesus – популярний сканер вразливостей з можливістю проведення атак і нейтралізації загроз після проведення сканування. Для його використання необхідно вибрати домен або IP-адресу яку використовуватимемо для проведення сканування на вразливості – використаємо домен seb.com (див.рис.3.3.6):

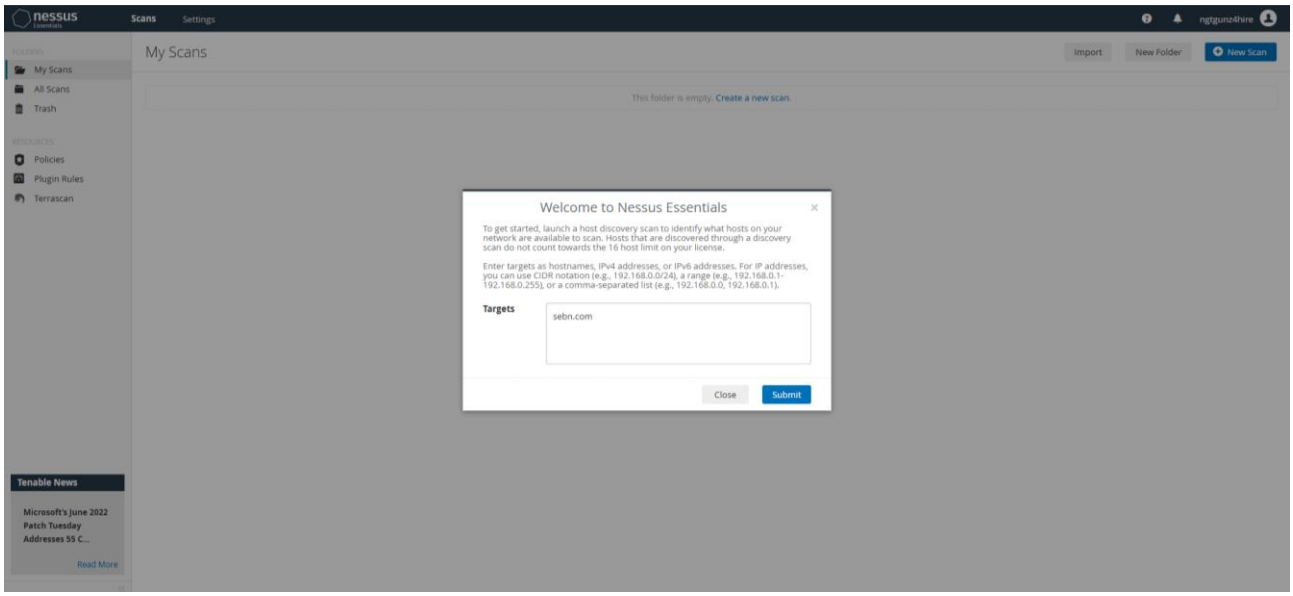

Рисунок 3.3.6 – Введення цілі для сканування

Після сканування отримуємо наступні результати (див.рис.3.3.7):

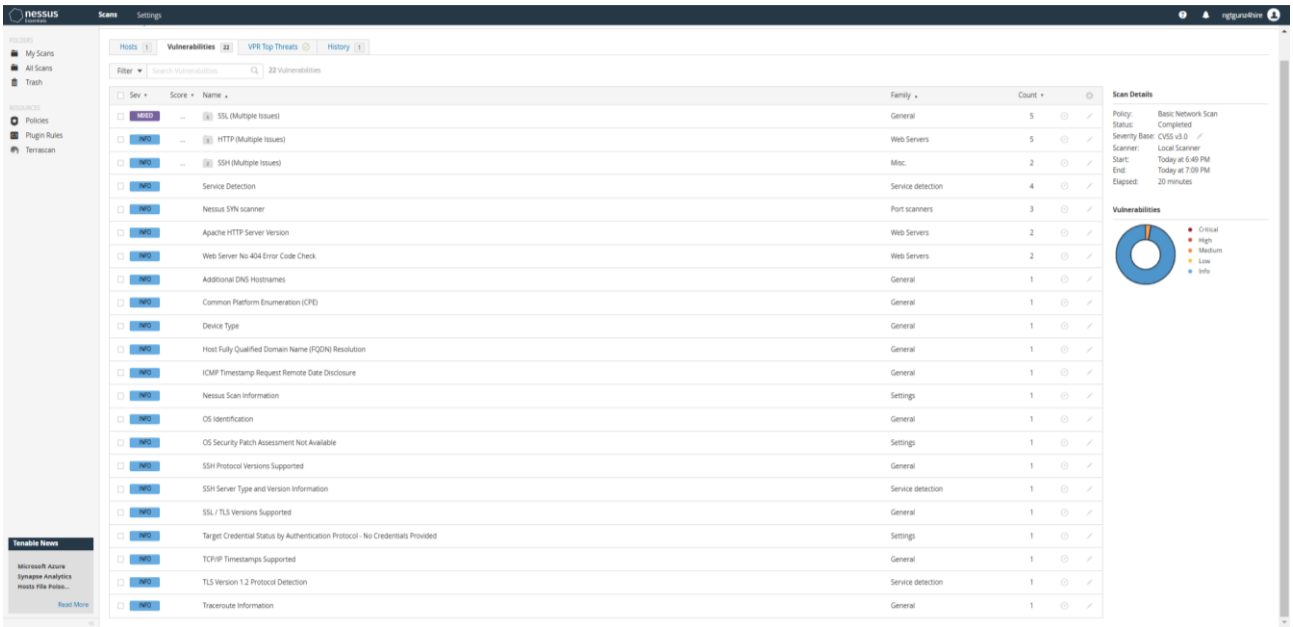

Рисунок 3.3.7 – Результат сканування

Проаналізуємо кожен з етапів сканування:

- Traceroute Information – у ньому циркулює домени через які проходить інформація для роботи sebn.com (див.рис.3.3.8):

Рисунок 3.3.8 – IP-адреси через які циркулює інформація

- TLS Version 1.2 Protocol Detection – виявлення версії протоколу криптографічного захисту TLS v1.2 (див.рис.3.3.9):

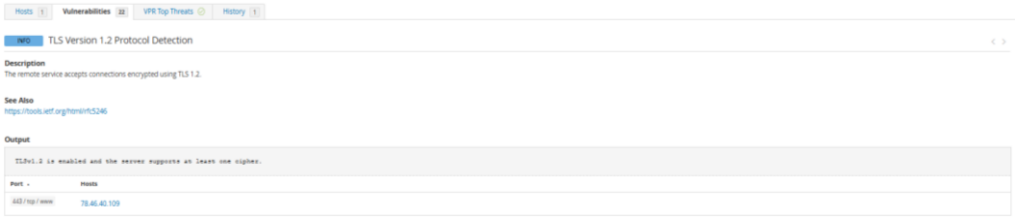

Рисунок 3.3.9 – Використання захищеного протоколу криптографічного захисту TLS v1.2

- SSH Server Type and Version Information – виявлення отримання віддаленого поступу через протокол SSH (див.рис.3.3.10):

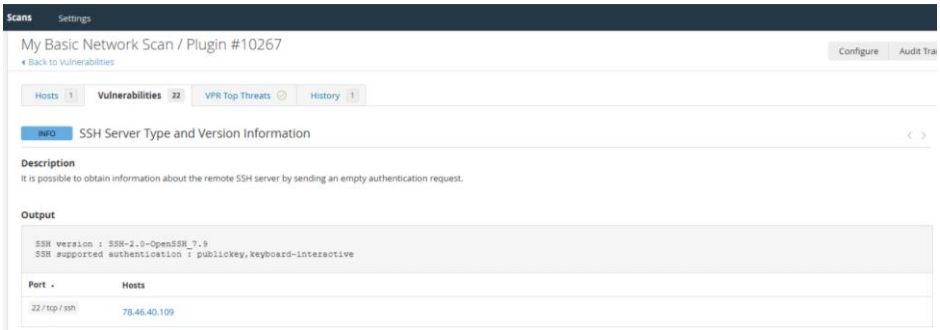

Рисунок 3.3.10 – Виявлення віддаленого доступу по SSH

- Service Detection – використання різних сервісів та портів для функціонування систем безпеки і віддаленого доступу (див.рис.3.3.11):

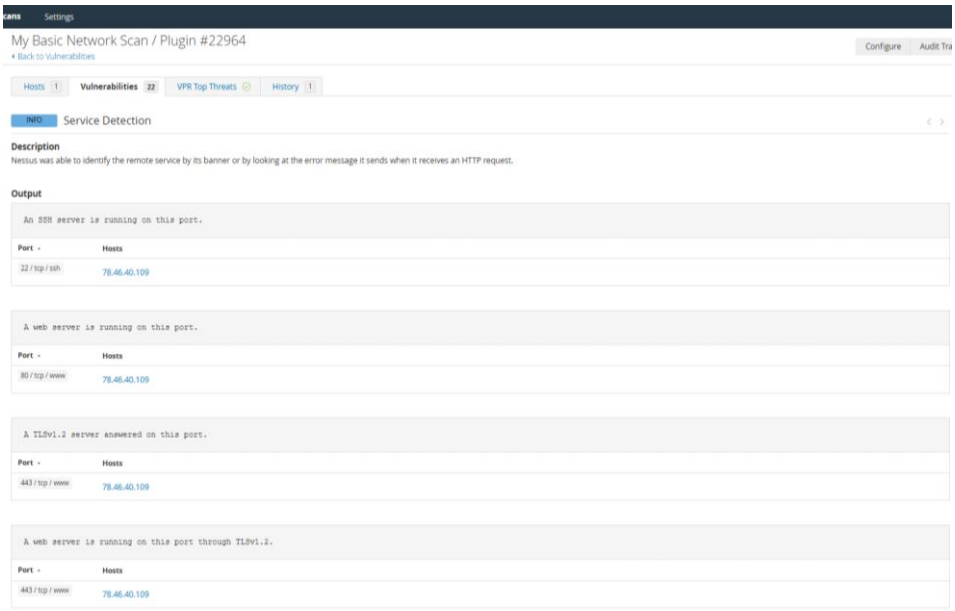

Рисунок 3.3.11 – Використання сервісів та портів для функціонування систем безпеки і віддаленого доступу

- Виявлення вразливості SSL Certificate Cannot Be Trusted (див.рис.3.3.12):

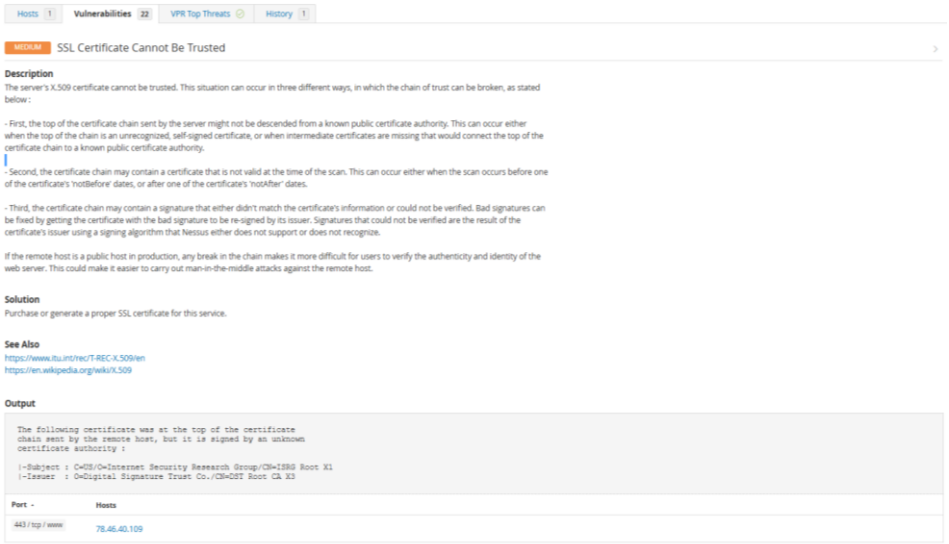

Рисунок 3.3.12 – Термін дії SSL сертифіката закінчився

Для нейтралізації вразливості необхідно згенерувати новий SSL сертифікат. Перейдемо до інструменту OWASP ZAP – з його використанням отримаємо можливість виявити вразливості напряму в самому домені sebn.com (див.рис.3.3.13):

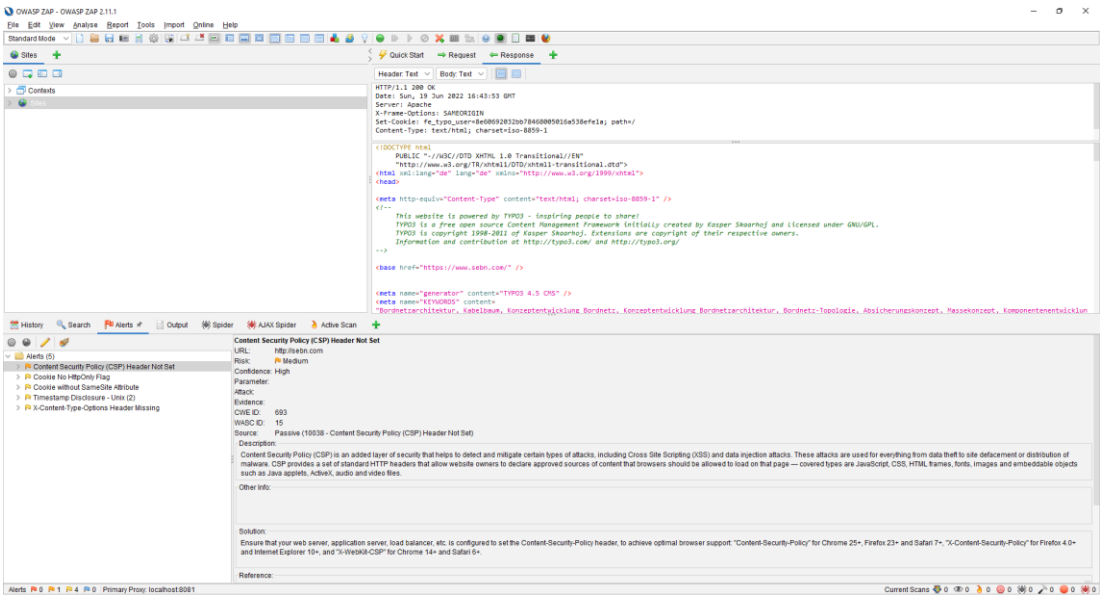

Рисунок 3.3.13 – Результат сканування OWASP ZAP

Вразливість Content Security Policy (CSP) дозволяє проводити XSS-атаки, і SQL-ін’єкції. Завдяки таким атакам є можливість отримання інформації з бази даних (логінів, паролів, електронних адрес) та іншого виду конфіденційної інформації.

Щоб таких вразливостей не було необхідно використовувати більш новітнє програмне забезпечення і проходити регулярні оновлення як апаратного так і програмного забезпечення. Перейдемо до наступної вразливості (див.рис.3.3.14):

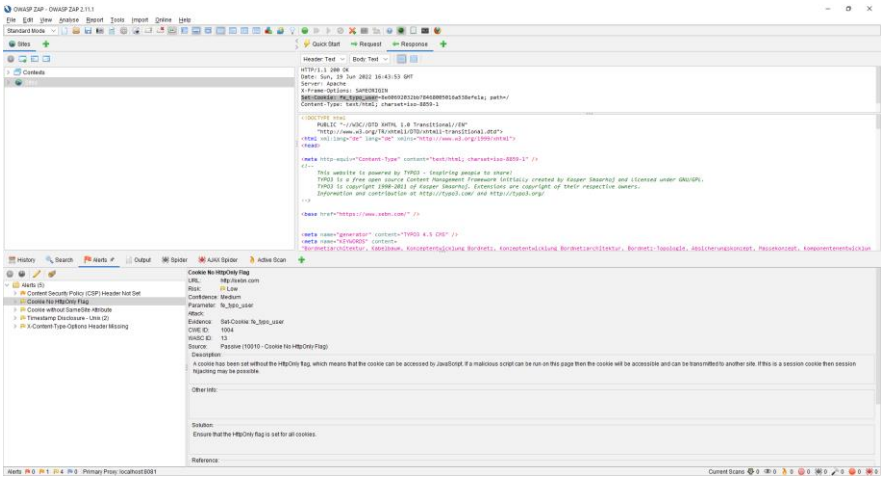

Рисунок 3.3.14 – Виявлення вразливості Cookie No HTTP Only Flag

Вразливість Cookie HTTP Only Flag дозволяє проводити атаку підміни cookie файлу з метою отримання (логіну, паролю, сесії входу і конфіденційну інформацію з веб-браузера користувача).

Для нейтралізації вразливості необхідно зменшити кількість cookie які не виконують свою функцію, або перевести їх на захищений протокол HTTPS.

Переходимо до вразливості Cookie without Same Site Attribute (див.рис.3.3.15):

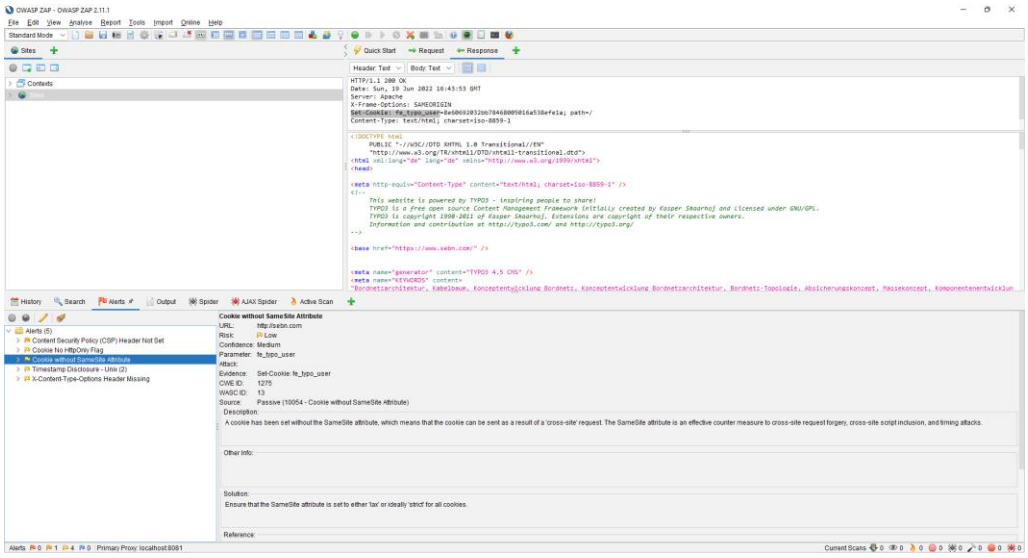

Рисунок 3.3.15 – Вразливість Cookie without Same Site Attribute

Вразливість Cookie without Same Site Attribute використовується для проведення атак ‘cross-site’ request для отримання запитів з сервера для проведення SQL-injection, XSS-attacks.

Для нейтралізації вразливості необхідно перевести атрибут Same Site в ‘strict’ для усіх файлів cookie.

Наступною вразливістю буде Timestamp Disclosure – Unix (див.рис.3.3.16):

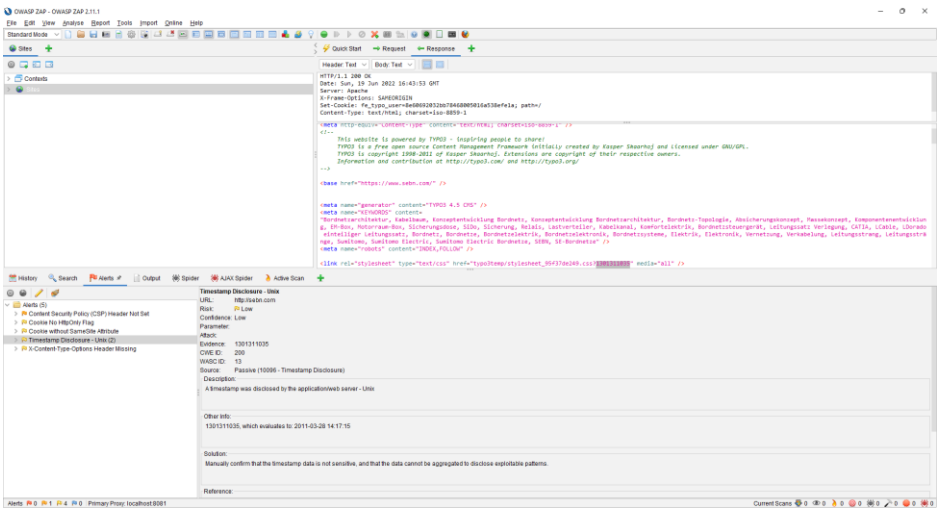

Рисунок 3.3.16 – Вразливість Timestamp Disclosure – Unix

Вразливість Timestamp Disclosure – Unix дозволяє маніпулювати часом або сесіями для підміни або видалення останніх сесій (приховувати свою присутність на сервері).

Для вирішення вразливості необхідно вручну або автоматично виставити тільки ті сесії або дії на сервері які не міститимуть важливої або інформації з обмеженим доступом.

Вразливість X-Content-Type-Options Header Missing (див.рис.3.3.17):

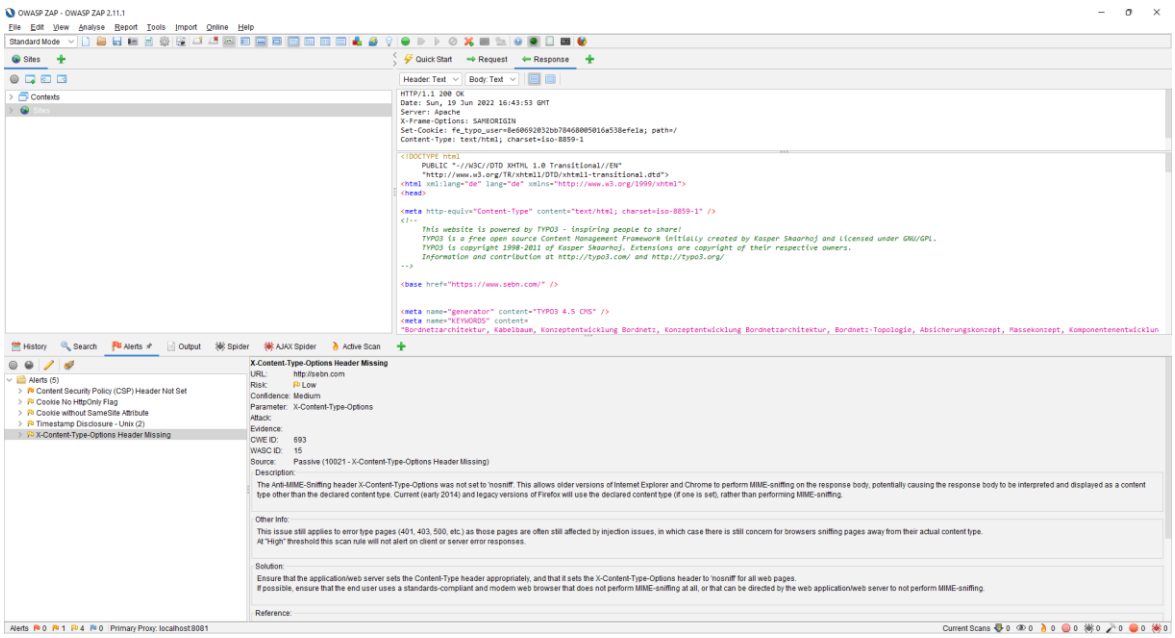

Рисунок 3.3.17 - Вразливість X-Content-Type-Options Header Missing

Вразливість X-Content-Type-Options Header Missing дозволяє перехоплювати трафік використовуючи інструменти для проведення sniffing-атак (збору інформації в каналі зв’язку). Щоб нейтралізувати вразливість необхідно змінити налаштування захисту в Content Security Policy (CSP) і налаштувати її з уникненням sniffing-атак.

Висновок: Для забезпечення належного захисту необхідно використовувати новітнє програмне забезпечення з останніми оновленнями систем інформаційної безпеки, також проводити регулярний аудит з навчання працівників з використанням програмного забезпечення.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ І ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці та безпека в надзвичайних ситуаціях

Охорона праці на підприємстві починається з організації управління охороною праці. Роботодавець зобов'язаний створити в кожному структурному підрозділі і на робочому місці умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Відповідальність за розроблення положень, типових інструкцій та інших нормативних документів з питань охорони праці та своєчасного доведення їх до відома працівників покладається на працівника, відповідального за безпеку праці та Профспілковий комітет.

Також до сфери їх компетенції відноситься відсторонення від роботи осіб, що не пройшли вступного та періодичних інструктажів з техніки безпеки. Контроль за дотриманням працівниками правил поводження із засобами механізації, автоматизації та іншим обладнанням, вимог інструкцій з охорони праці та техніки безпеки у відповідності до Закону України «Про охорону праці» здійснюється особою, відповідальною за безпеку праці.

Фінансування профілактичних заходів з охорони праці, виконання загальнодержавної, галузевих та регіональних програм поліпшення стану безпеки, гігієни праці та виробничого середовища, інших державних програм, спрямованих на запобігання нещасним випадкам та професійним захворюванням, передбачається, поряд з іншими джерелами фінансування, визначеними законодавством, у державному і місцевих бюджетах.

Для підприємств, незалежно від форм власності, або фізичних осіб, які використовують найману працю, витрати на охорону праці становлять не менше 0,5 відсотка від суми реалізованої продукції.

На підприємствах, що утримуються за рахунок бюджету, витрати на охорону праці передбачаються в державному або місцевих бюджетах і становлять не менше 0,2 відсотка від фонду оплати праці. Суми витрат з охорони праці, що належать до

валових витрат юридичної чи фізичної особи, яка відповідно до законодавства використовує найману працю, визначаються згідно з переліком заходів.

Оцінка стану охорони праці установи Оцінка стану охорони праці на підприємстві в цілому і в його структурних підрозділах базується на аналізі даних атестації робочих місць, паспортизації санітарно-технічного стану цехів та відділів, результатах виконання комплексних планів покращення умов праці та санітарнооздоровчих заходів, а також на динаміці показників виробничого травматизму та професійних захворювань. Оцінка стану охорони праці та пільги і компенсація кожного робочого місця, а також аналізу записів в журналі трьох-ступеневого контролю охорони праці.

Порушеннями правил вважаються: робота без інструктажу або його термін прострочений; робота без засобів захисту, передбачених інструкцією з техніки безпеки; робота на обладнанні, що не пройшло технічного огляду, або його термін прострочений; невідповідність прийомів праці вимогам інструкції з техніки безпеки та ін.

При підрахунках встановлюється перелік основних вимог безпеки до виробничого обладнання, що подані в державних та галузевих стандартах. Порушенням вимоги безпеки вважається відсутність або зіпсованість передбачених технічною документацією засобів захисту (блокування, огородження, сигналізації), засобів електрозахисту, засобів автоматичного або ручного управління, зміни в конструкції, не передбачені технічною документацією та ін.

Охоронно-пожежна сигналізація управляється приймально контрольними приладами, який здійснює живлення передавачів по шлейфах охоронно-пожежної сигналізації, прийом тривожних повідомлень від передавачів, а також передає їх на станцію централізованого спостереження і формує сигнали тривоги на спрацьовування інших складових.

У приміщенні диспетчерського пункту та інших місцях розміщення приладів сигналізації та вузлів керування знаходиться наказ про порядок дії чергового персоналу в разі появи індикаторів пожежі або несправності УПС (управління пожежної сигналізації).

4.2 Аналіз складових потенційної небезпеки, оцінка рівня події та визначення безпосередньої причини події

Для того щоб проявилась шкода джерела потенційної небезпеки, потрібен конкретний вражаючий фактор, який власне і призводить до збитків.

Під вражаючими факторами розуміють такі чинники життєвого середовища, які за певних умов завдають шкоди як людям, так і системам життєзабезпечення людей, призводять до матеріальних збитків.

Класифікація вражаючних факторів:

За своїм походженням вражаючі фактори можуть бути:

- фізичні (в тому числі енергетичні);
- хімічні;
- біологічні;
- психофізіологічні;
- соціальні.

Залежно від наслідків впливу конкретних вражаючих факторів на організм людини вони в деяких випадках (наприклад, в охороні праці) поділяються на шкідливі та небезпечні [22, с. 118].

Шкідливими факторами прийнято називати такі чинники життєвого середовища, які призводять до погіршення самопочуття, зниження працездатності, захворювання і навіть до смерті як наслідку захворювання.

Небезпечними факторами називають такі чинники життєвого середовища, які призводять до травм, опіків, обморожень, інших пошкоджень організму або окремих його органів і навіть до раптової смерті.

Хоча поділ вражаючих факторів на небезпечні та шкідливі досить умовний, бо інколи неможливо віднести який-небудь фактор до тієї чи іншої групи, він ефективно використовується в охороні праці для організації розслідування та обліку нещасних випадків та професійних захворювань, налагодження роботи, спрямованої на розробку заходів і засобів захисту працівників, профілактику травматизму та захворюваності на виробництві.

Безпека є відносним поняттям. Абсолютної безпеки для всіх обставин та умов не існує.

Просте запитання: «Яка безпека є достатньою?» не має простої Аналіз небезпек починають з попереднього дослідження, яке дозволяє в основному ідентифікувати джерела небезпек.

Потім, при необхідності, дослідження можуть бути поглиблені і може бути виконаний детальний якісний аналіз. Методи цих аналізів та прийоми, які використовуються при їх виконанні, відомі під різними назвами.

Нижче наведені основні з цих загальних інструментів [18, с. 135]. Попередній аналіз небезпек — це аналіз загальних груп небезпек, присутніх в системі, їх розвитку та рекомендації щодо контролю.

ПАН є першою спробою в процесі безпеки систем визначити та класифікувати небезпеки, які мають місце в системі.

ПАН звичайно виконується у такому порядку:

- вивчають технічні характеристики об'єкта, системи чи процесу, а також джерела енергії, що використовуються, робоче середовище, матеріали, встановлюють їхні небезпечні та шкідливі властивості;
- визначають закони, стандарти, правила, дія яких поширюється на даний об'єкт, систему чи процес;
- перевіряють технічну документацію на відповідність її законам, правилам, принципам і нормам безпеки;
- складають перелік небезпек, в якому зазначають ідентифіковані джерела небезпек (системи, підсистеми, компоненти), чинники, що викликають шкоду, потенційні небезпечні ситуації, виявлені недоліки.

При проведенні ПАН особливу увагу приділяють наявності вибухопожежнонебезпечних та токсичних речовин, виявленню компонентів об'єкта, в яких можлива їх присутність, потенційна небезпечна ситуація від неконтрольованих реакцій чи при перевищенні тиску [27, с. 19].

Після того, як виявлені крупні системи об'єкта, які є джерелами небезпеки, їх можна розглядати окремо і досліджувати більш детально за допомогою інших методів аналізу.

4.3 Основні заходи щодо підвищення стійкості роботи, які здійснюються на об’єкті завчасно, за сигналами оповіщення ЦЗ та при раптовому виникненні НС

Оцінка стійкості роботи об’єкта – це всебічне вивчення підприємства з погляду здатності його протистояти впливу вражаючих факторів ядерного вибуху, відновлення виробництва при одержанні середніх і слабких руйнувань.

Мета дослідження складається в тому, щоб виявити уразливі місця в роботі об’єкта у воєнний час і виробити найбільш ефективні пропозиції і рекомендації, спрямовані на підвищення його стійкості.

Надалі ці рекомендації включаються в план заходів щодо підвищення стійкості роботи об’єкта, що і реалізується. Дослідження стійкості підприємств проводиться силами інженерно-технічного персоналу із залученням фахівців науково-дослідних і проектних організацій, пов’язаних із даним підприємством. Організатором і керівником дослідження є керівник підприємства – начальник ЦО об’єкта.

Основними документами для організації дослідження стійкості роботи об’єкта є: наказ керівника підприємства; календарний план основних заходів щодо підготовки до проведення дослідження; план проведення дослідження. Дослідження стійкості повинне вестися творчо з урахуванням специфічних особливостей виробництва.

Від підсумків дослідження залежить планування і проведення в життя економічно обґрунтованих заходів ЦО, спрямованих на підвищення стійкості роботи об’єкта народного господарства. Підвищення стійкості роботи об’єкта народного господарства є складною задачею, що вимагає великих матеріальних витрат і постійної уваги з боку всіх органів ЦО.

Для підвищення протипожежної стійкості проводяться профілактичні заходи як для запобігання пожеж, так і для створень умов, що утрудняють поширення вогню і полегшують боротьбу з ним у вогнищах виникнення.

Це забезпечується шляхом: підвищення вогнестійкості різних конструкцій (особливо дерев’яних); створенням мережі водойм на території об’єктів устаткування під’їздів до рік, озер, ставків; створення площадок для пожежної техніки; захист у відкритих технологічних установок; зменшення на виробництві

до технологічно обґрунтованого мінімуму легкозаймистих матеріалів; зміною технологій, що виключають застосування вогненебезпечних і вибухонебезпечних речовин; застосування автоматичних ліній засобів гасіння пожеж; усунення умов, що створюють вибухові суміші в будинках; пристрій аварійних заглиблених ємностей для швидкого зливу з технологічного устаткування пальних рідин.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було проведено аудит інформаційної безпеки, виявлення й нейтралізація вразливостей виявленні програмними засобами для проведення аудиту. Методи й заходи протидії загрозам, що дозволяють мінімізувати вплив на основі безпеки інформації (цілісності, доступності, конфіденційності).

Формування аудиту інформаційної безпеки розпочинається з планування і аналізу. В першу чергу аналізуються сервіси які будуть використовуватися в процесі обробки, наступним етапом є оцінка ризиків пов’язана з використанням сервісів. Після чого забезпечується заходи для зниження впливу або повної нейтралізації вразливості.

На підставі отриманих даних, що були отримані на етапі проведення аудиту розроблено план з нейтралізації загроз або мінімізація їх впливу.

Були обрані найоптимальніші рішення з унеможливленням виникнення потенційних вразливостей в подальшому, а також вказано доцільність їх нейтралізації.

Результатом роботи було проведено аудит інформаційної безпеки для підприємства ТОВ «СЕ Борднетце-Україна».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Auditorías De Ciberseguridad [Електронний ресурс] – Режим доступу: https://campusetic.com/auditorias-de-ciberseguridad/

2. Holistic IT Governance, Risk Management, Security and Privacy [Електронний ресурс] – Режим доступу: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/holistic-it-governance-risk-management-security-and-privacy-needed-for-effective-implementation-and

3. What is IT Compliance? [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/us/threat-reference/it-compliance

4. What Are The IT Security Compliance Standards? [Електронний ресурс] – Режим доступу: https://www.seaglasstechnology.com/what-are-the-it-security-compliance-standards/

5. How to Pass an IT Compliance Audit? [Електронний ресурс] – Режим доступу: https://www.ekransystem.com/en/blog/how-to-pass-it-compliance-audit

6. DNSDumpster – Information Gathering with DNSDumpster [Електронний ресурс] – Режим доступу: https://thedarksource.com/information-gathering-with-dnsdumpster/

7. What Is Shodan? How to Use It & How to [Електронний ресурс] – Режим доступу: https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/

8. Верига Ю.А. Звітність підприємств: навчальний посіб. / Ю. А. Верига ; Мін-во освіти і науки України, КНЕУ. – К. : КНЕУ, 2015. – 322 с.

9. Волошин Д. Методологические основы внутреннего аудита еффективности системи управленческого учета на предприятии / Д.Волошин // Проблеми теории и практики управления. – 2012. № 1. – С.49-58.

10. Гандзюк М.П. Основи охорони праці: Підручник. / М.П. Гандзюк, Є.П.Желібо, М. О.Халімовський. – К.: Каравела, 2008. – 548 с.

Додаток А

Мережа DNS-серверів філій SEBN

Hostname	IP Address	T	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title	HTTPS / Title	FTP / SSH / Telnet	HTTP Other
citrix.sebn.com	62.225.134.98	A		DTAG Internet service provider operations	Germany			CN: .sebn.com		
mdm01.sebn.com	62.176.233.36	A	customer-pool2-36.wobline-ip.de	WOBCOM	Germany			server title: 302 Found CN: .sebn.com		server
mdm03.sebn.com	62.176.233.45	A	customer-pool2-45.wobline-ip.de	WOBCOM	Germany					
guestwifi.sebn.com	1.1.1.1	A	one.one.one.one	CLOUDFLARENET	Australia		cloudflare title: 301 Moved Permanently	cloudflare CN: cloudflare-dns.com O: Cloudflare Inc		
hatpbxsb01.sebn.com	62.225.134.102	A		DTAG Internet service provider operations	Germany					
www.sebn.com	78.46.40.109	A	static.109.40.46.78.clients.your-server.de	HETZNER-AS	Germany		Apache title: 301 Moved Permanently	Apache title: 301 Moved Permanently CN: sebn.com	ftp: 220 (vsFTPd 2.3.4) ssh: SSH-2.0-OpenSSH_7.9	
mdm02.sebn.com	62.176.233.37	A	customer-pool2-37.wobline-ip.de	WOBCOM	Germany					
hatmx00001.sebn.com	62.176.233.35	A	hatmx00001.sebn.com	WOBCOM	Germany					
gormx00001.sebn.com	81.15.209.126	A	gormx00001.sebn.com	ASN-TELENERGO ul. PERKUNA 47, WARSZAWA	Poland					
ns31.domaincontrol.com.	97.74.105.16	NS	ns31.domaincontrol.com	GODADDY-DNS	United States					
ns32.domaincontrol.com.	173.201.73.16	NS	ns32.domaincontrol.com	GODADDY-DNS	United States					
10 sebn-com.mail.protection.outlook.com.	104.47.23.138	MX	mail-tycjpn010138.inbound.protection.outlook.com	MICROSOFT-CORP-MSN-AS-BLOCK	Japan					
30 gormx00001.sebn.com.	81.15.209.126	MX	gormx00001.sebn.com	ASN-TELENERGO ul. PERKUNA 47, WARSZAWA	Poland					
20 hatmx00001.sebn.com.	62.176.233.35	MX	hatmx00001.sebn.com	WOBCOM	Germany					