Лабораторна робота № 3(2.1.9)

Вимоги щодо відповідності та місцеві обмеження

Хід роботи:

Частина 1: Дослідження компаній з пентестингу для відповідності регуляторним вимогам

Компанія № 1: Coalfire

Назва компанії: Coalfire

Веб-сайт: https://www.coalfire.com

Для яких доменів відповідності компанія надає послуги тестування на проникнення? Перелічіть домени та дайте короткий опис фокусу кожного:

Coalfire спеціалізується на наданні послуг пентестингу для широкого спектра регуляторних фреймворків:

PCI DSS (Payment Card Industry Data Security Standard) – тестування безпеки платіжних систем для організацій, які обробляють дані платіжних карток. Coalfire проводить щорічні внутрішні та зовнішні тести на проникнення відповідно до вимог стандарту.

FedRAMP (Federal Risk and Authorization Management Program) – програма федеральної авторизації для хмарних сервісів. Coalfire є провідною організацією 3PAO (Third Party Assessment Organization), яка проводить оцінку безпеки хмарних провайдерів, що працюють з федеральними агенціями США.

HITRUST – комплексний фреймворк для охорони здоров'я. Coalfire допомагає медичним організаціям досягти сертифікації HITRUST через тестування безпеки та оцінку контролів.

ISO 27001 – міжнародний стандарт управління інформаційною безпекою. Coalfire проводить аудити та тестування для підтвердження відповідності системам управління інформаційною безпекою.

SOC 2 (Service Organization Control 2) – звіти про контролі безпеки, доступності та конфіденційності для сервісних організацій.

CMMC (Cybersecurity Maturity Model Certification) – сертифікація кібербезпеки для підрядників Міністерства оборони США, особливо для рівня 3.

Які ресурси знань щодо фреймворків відповідності доступні на веб-сайті компанії?

Coalfire надає різноманітні ресурси знань:

Щорічний звіт про тестування на проникнення (4th Annual Penetration Test Report), який аналізує понад 3,100 тестів на проникнення від майже 1,600 клієнтських проектів у технологічному, фінансовому, медичному та роздрібному секторах.

Технічні документи та дослідження з FedRAMP, PCI DSS, CMMC та інших фреймворків відповідності

Платформа Coalfire Compliance Essentials, яка координує оцінки в межах понад 85 фреймворків і зменшує ручні зусилля на 40%.
Вебінари та навчальні матеріали з питань відповідності та кібербезпеки.

Хто є основними клієнтами компанії (перелічіть принаймні трьох)?

Coalfire обслуговує понад 6,000 клієнтів по всьому світу, включаючи:
П'ять найбільших хмарних провайдерів (включаючи AWS, Google Cloud, Microsoft Azure)
Premera Blue Cross – великий медичний страховик
Truework – технологічна компанія
Effectual – постачальник хмарних послуг
Організації в фінансових послугах, охороні здоров'я, роздрібній торгівлі, технологічному секторі та державних установах

Які нагороди або визнання отримала компанія?

Coalfire отримала численні нагороди:
Editor's Choice for Penetration Testing від Cyber Defense Magazine (2023)
Hot Company for Vulnerability Management від Cyber Defense Magazine (2023)
Most Innovative for Vulnerability Assessment, Remediation, and Management від Cyber Defense Magazine (2023)
№1 у відповідності, FedRAMP та тестуванні на проникнення хмарних систем
Визнана найбільшою у світі компанією, що спеціалізується виключно на послугах кібербезпеки

Компанія № 2: Prescient Security

Назва компанії: Prescient Security & Assurance
Веб-сайт: https://prescientsecurity.com

Для яких доменів відповідності компанія надає послуги тестування на проникнення? Перелічіть домени та дайте короткий опис фокусу кожного:

Prescient Security надає послуги тестування на проникнення для понад 25 фреймворків відповідності:
SOC 2 Type I та Type II – оцінка контролів безпеки, доступності, цілісності обробки, конфіденційності та приватності для сервісних організацій.
ISO 27001/27701/42001 – міжнародні стандарти для систем управління інформаційною безпекою, управління приватністю та управління штучним інтелектом.
HIPAA (Health Insurance Portability and Accountability Act) – регуляторні вимоги для захисту медичної інформації в сфері охорони здоров'я.
PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних індустрії платіжних карток для організацій, що обробляють платіжну інформацію.
GDPR (General Data Protection Regulation) – європейський регламент захисту даних, який регулює обробку персональних даних громадян ЄС.
FedRAMP – програма федеральної авторизації для хмарних сервісів, що працюють з урядом США.
HITRUST – комплексний фреймворк безпеки для індустрії охорони здоров'я.
CMMC (Cybersecurity Maturity Model Certification) – модель зрілості кібербезпеки для підрядників Міністерства оборони США.

Які ресурси знань щодо фреймворків відповідності доступні на веб-сайті компанії?
Prescient Security надає різноманітні ресурси:
Детальні описи понад 25 фреймворків відповідності з роз'ясненням вимог та процесів сертифікації.
Методології тестування на основі OWASP Top 10, API Security Top 10, NIST 800-115 та OSSTMM.
Інструмент Cacilian – власна платформа для управління процесом тестування на відповідність від планування до звітності.
Блог з актуальними статтями про оновлення стандартів (наприклад, PCI DSS 4.0).
Вебінари з експертами з питань кібербезпеки та відповідності.
Хто є основними клієнтами компанії (перелічіть принаймні трьох)?
Prescient Security обслуговує понад 5,000 клієнтів по всьому світу, зокрема:
Компанії SaaS (Software as a Service), особливо в сферах технологій, фінансів та охорони здоров'я
PrimeRx Enterprise – провайдер фармацевтичного програмного забезпечення
Vectorize AI, Inc – компанія штучного інтелекту
Стартапи та середні підприємства, що прагнуть досягти сертифікації SOC 2, ISO 27001 та інших стандартів
Які нагороди або визнання отримала компанія?
Prescient Security отримала визнання як:
Глобальна топ-20 незалежна компанія з аудиту та тестування на проникнення
Сертифікація CREST (Council of Registered Ethical Security Testers) – міжнародне визнання технічної компетентності в етичному хакінгу
PCI QSA (Qualified Security Assessor) – кваліфікований оцінювач безпеки платіжних систем
FedRAMP 3PAO (Third-Party Assessment Organization) – авторизована організація для оцінки безпеки федеральних хмарних систем
Позитивні відгуки клієнтів про професіоналізм, якість обслуговування та експертизу
Компанія № 3: Rapid7
Назва компанії: Rapid7
Веб-сайт: https://www.rapid7.com
Для яких доменів відповідності компанія надає послуги тестування на проникнення? Перелічіть домени та дайте короткий опис фокусу кожного:
Rapid7 надає послуги тестування на проникнення для широкого спектру регуляторних вимог:
PCI DSS – щорічне тестування мережі для організацій, що обробляють платіжні картки. Rapid7 проводить як зовнішні, так і внутрішні тести на проникнення відповідно до вимоги 11 стандарту.
HIPAA – оцінка безпеки для організацій охорони здоров'я, що обробляють захищену медичну інформацію (PHI).
GDPR – допомога організаціям у дотриманні європейських вимог щодо захисту персональних даних через виявлення вразливостей.

SOC 2 – тестування контролів безпеки для сервісних організацій.
ISO 27001 – підтримка організацій у досягненні сертифікації через регулярне тестування та оцінку безпеки.
GLBA (Gramm-Leach-Bliley Act) – вимоги до фінансових установ щодо захисту конфіденційних даних клієнтів.

Які ресурси знань щодо фреймворків відповідності доступні на веб-сайті компанії?

Rapid7 надає багато ресурсів для навчання та підтримки відповідності:
Розділ Security Compliance Solutions з детальною інформацією про різні стандарти та регуляції.
Metasploit – найбільш використовуваний у світі інструмент для тестування на проникнення з відкритим кодом, який активно підтримується Rapid7.
Дослідницькі звіти та аналітику загроз, включаючи квартальні звіти про ландшафт загроз.
InsightVM, InsightIDR та InsightCloudSec – платформи для управління вразливостями, виявлення загроз та безпеки хмарних середовищ.
Вебінари, блоги та навчальні матеріали з тем кібербезпеки та відповідності.

Хто є основними клієнтами компанії (перелічіть принаймні трьох)?

Rapid7 обслуговує понад 11,000 клієнтів по всьому світу, включаючи:
Domino's Pizza – компанія використовує послуги Rapid7 для симуляції атак, тестування на проникнення та реагування на інциденти
Hormel Foods – використовує рішення Rapid7 для захисту своєї IT-інфраструктури
Johnson & Johnson – компанія працює з Rapid7 для вбудовування покращених процесів безпеки в цикли розробки продуктів
Maximus – використовує платформу Rapid7 для управління кіберризиками в публічних хмарних середовищах
Bob's Stores – використовує рішення Rapid7 як основу своєї програми безпеки
Організації в технологічному, телекомунікаційному, медичному, фінансовому, страховому, роздрібному секторах, вищій освіті та державних установах

Які нагороди або визнання отримала компанія?

Rapid7 отримала численні нагороди та визнання:
Security Vendor of the Year на CRN Channel Awards 2024
Excellence in Workplace Health and Wellbeing на Belfast Telegraph IT Awards
Best SIEM Solution від SC Awards Europe 2024
Best Vulnerability Management Solution (InsightVM) від SC Awards 2023
Best Threat Detection Technology (InsightIDR) від SC Awards 2023
Security Analytics та Application Security категорії на Cybersecurity Excellence Awards 2016
One of Boston Business Journal's Best Places to Work 2023

Reflection (Рефлексія)

Питання: Чи повинні компанії у вашій країні дотримуватися фреймворків відповідності, що накладаються іншими країнами? Якщо так, які наслідки недотримання вимог цих фреймворків та які штрафи передбачені у разі витоку даних?

Відповідь:

Так, українські компанії повинні дотримуватися міжнародних фреймворків відповідності, особливо якщо вони працюють з європейськими або американськими клієнтами. Ключові аспекти:

1. GDPR (General Data Protection Regulation)

Українські компанії, які обробляють персональні дані громадян ЄС, зобов'язані дотримуватися GDPR. Це особливо актуально для:

IT-компаній та розробників програмного забезпечення, які працюють з європейськими клієнтами

Аутсорсингових центрів, які обробляють дані від європейських компаній

Будь-яких організацій, що надають послуги або продають товари громадянам ЄС

Наслідки недотримання GDPR:

Штрафи до €20 мільйонів або до 4% від річного глобального обороту компанії (обирається більша сума)

Втрата довіри клієнтів та репутаційні збитки

Можливість призупинення обробки даних або заборона передачі даних з ЄС

Позови від постраждалих осіб

2. Українське законодавство про захист персональних даних

Україна має власний Закон України "Про захист персональних даних" від 1 червня 2010 року, який базується на Конвенції 108 Ради Європи. Проте наразі він не повністю відповідає стандартам GDPR.

У листопаді 2024 року Верховна Рада прийняла законопроєкт № 8153 "Про захист персональних даних", який гармонізує українське законодавство з GDPR та Конвенцією 108+. Новий закон передбачає:

Штрафи до 5% від річного обороту компанії за найсерйозніші порушення

Обов'язок повідомляти про витоки даних контролюючий орган та постраждалих осіб протягом 72 годин

Призначення посадових осіб з захисту даних (DPO) у певних випадках

Проведення оцінки впливу на захист даних (DPIA) для високоризикової обробки

Поточні санкції за українським законодавством:

Адміністративні штрафи від €170 до €425 (відносно невеликі порівняно з GDPR)

Кримінальна відповідальність для фізичних осіб за незаконне збирання, зберігання та поширення конфіденційної інформації (стаття 182 Кримінального кодексу України)

3. Інші міжнародні стандарти

Українські компанії, що працюють з міжнародними клієнтами, також можуть бути зобов'язані дотримуватися:

PCI DSS – для обробки платіжних карток

SOC 2 – для постачальників хмарних послуг

ISO 27001 – міжнародний стандарт інформаційної безпеки
HIPAA – якщо обробляються медичні дані американських пацієнтів

4. Контекст євроінтеграції України

Як країна-кандидат на вступ до ЄС, Україна зобов'язалася гармонізувати своє законодавство з європейськими стандартами, включаючи GDPR. Це означає, що вимоги до захисту персональних даних будуть тільки посилюватися.

Висновок: У ході виконання лабораторної роботи було досліджено три провідні компанії з пентестингу (Coalfire, Prescient Security та Rapid7), які надають послуги для забезпечення відповідності міжнародним регуляторним вимогам. Встановлено, що українські компанії, особливо в IT-секторі, зобов'язані дотримуватися міжнародних стандартів відповідності при роботі з іноземними клієнтами. Недотримання вимог може призвести до серйозних фінансових санкцій (штрафи до 5% річного обороту в Україні та до €20 мільйонів або 4% глобального обороту згідно GDPR), втрати репутації та міжнародних клієнтів. З урахуванням євроінтеграційних процесів, регулярне тестування на проникнення та аудити безпеки стають критично важливими інструментами для українських компаній у забезпеченні відповідності та захисту інформації.