УДК 004.056
DOI: 10.31673/2409-7292.2021.020708

Галузін І.С., Найман Г.Г.

УПРАВЛІННЯ УРАЗЛИВОСТЯМИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ РІШЕНЬ QUALYS

У статті проаналізовано проблему забезпечення кібербезпеки корпоративних інформаційних систем та визначено мету та завдання їх захисту. Проведено аналіз технології управління вразливостями корпоративних інформаційних систем. Досліджено методи та засоби управління вразливостями корпоративних інформаційних систем на базі рішення Qualys. Визначено призначення, основні функції та склад програмного забезпечення рішення Qualys. Розроблено варіант управління вразливостями корпоративної інформаційної системи на базі рішення Qualys.

Ключові слова: Корпоративна інформаційна система, кібербезпека, управління вразливостями, рішення qualys, qualys cloud agent, ризик.

Вступ

Ведення сучасного бізнесу передбачає використання корпоративних систем обробки і надання інформації. У той же час, факт наявності конференційних даних в таких системах та необхідності їх циркулювання між користувачами актуалізує проблематику забезпечення захисту інформації. Встановлено, що використання вразливостей в інформаційних системах дозволяє акторам загроз отримати з них конференційні дані, що спричиняє фінансові втрати підприємствам. Впровадження технології управління вразливостями дозволить мінімізувати ризики компрометації інформаційних систем або наддасть дійсні аргументи щодо його прийняття. Такий підхід оптимізує фінансові витрати на технічні засоби захисту інформації та зробить підприємство біль захищеним від кібератак в цілому.

У роботі розглядається практичне використання технології управління вразливостями з використанням технічних засобів від вендора Qualys, який на момент написання роботи являється одним з найбільших постачальників послуг в даній сфері, позиціонується як один з лідерів і здатен задовільнити потребам навіть великої корпорації.

Актуальність проблеми

Нещодавно у звіті про розслідування порушень даних Verizon було проаналізовано 41 686 підтверджених випадків безпеки. У звіті було встановлено, що чіткий акцент робився на фінансовій вигоді [1]. IBM Security виявила, що середня вартість порушення даних становить 3,86 мільйона доларів для організації [2]. Авжеж бувають більш серйозні випадки. Наприклад в 2017 році агентство сповіщення про споживчі кредити Equifax оголосило, що стало жертвою кібератаки, в якій отримали доступ до персональних даних 145,5 мільйонів осіб. Це обійшлося організації більш ніж 575 мільйонів доларів [3].

Аналіз публікацій

Згідно 20 Critical Security Controls, випущеним Center for Internet Security, одним з п'яти найбільш важливих елементів управління для усунення переважної більшості вразливостей організації є «постійне оцінювання вразливостей і їх усунення» [4]. Традиційні технології безпеки, такі як антивірусне програмне забезпечення, брандмауер, системи запобігання вторгненню, VPN, являються необхідними засобами забезпечення безпеки корпоративних інформаційних систем. Проте, хоча вони ефективні у власних сферах призначення, жоден із цих заходів в повній мірі не виконує цієї умови. У цьому сенсі впровадження технології управління вразливостями є основою ефективної програми безпеки для посилення захисту організації.

Вибір вендора для ведення технології управління вразливостями являється важливим завданням для організації, бо надавані послуги, такі як мережевий сканер або інструменти звітності можуть не задовільнити її потребам. В цій роботі буде розглядатися рішення Qualys, оскільки компанія по дослідженню ринку The Forrester Wave відзначає цього вендора, як одного з лідерів, що здатен обробляти сканування великих гібридних IT-середовищ і що просуває ринок уперед [5]. Довідки клієнтів також вказують, що Qualys є

прекрасним вибором для сканування складних корпоративних середовищ і це підтверджується платформую для оцінки IT-продуктів Gartner peer insights [6].

Технологія управління уразливостями на базі рішення Qualys

Технологія управління уразливостями являється новим підходом в області кібербезпеки і в нормативних актах ще не має чіткого виділення етапів її створення. У той же час, є безліч практичних рекомендацій щодо її ведення від провідних компаній світу. Проаналізувавши цю інформацію, можна виділити наступний повторюваний цикл:

1. інвентаризація активів;
2. сканування активів мережевим сканером вразливостей;
3. сканування веб-додатків;
4. фаза звітування;
5. планування та оптимізація сценарію виправлення.

Інвентаризація активів. Активи підприємства – це сервери, настільні комп'ютери, копіювальні машини, мобільні пристрої тощо. Організації, як правило, проходять через безліч злиттів, поглинань і нових технологій. На жаль, ці обставини часто залишають компанії в омані щодо їх належної інвентаризації, і багато хто з них не в змозі ідентифікувати всі свої активи, які вимагають певного рівня захисту. Занадто часто компанії мають безліч невідомих активів в своєму середовищі, які можуть поставити під загрозу їхню безпеку в довгостроковій перспективі. Виявлення активів не є одноразовим елементом оцінки вразливості системи безпеки – це постійний процес, оскільки активи часто додаються та вилучаються з корпоративних мереж.

У Qualys процес ідентифікації активів починається автоматично на початку сканування. Під час нього технологічне рішення VM створює базу даних усіх комп’ютерних систем та пристроїв з IP-адресами, які приєднані до мережі. На рисунку 1. наведено приклад такої мережі [7]. Зазвичай пошук активів починається з введення у сканері певного діапазону IP-адрес або домену.

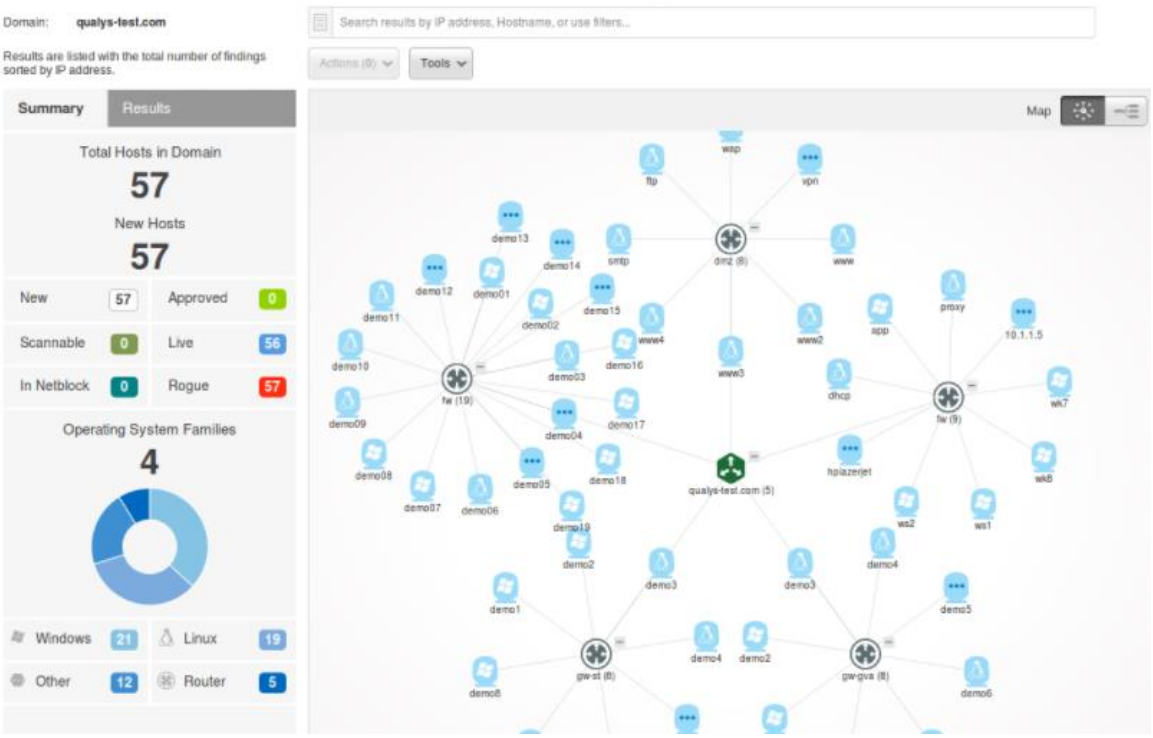

Рис. 1. Приклад групи активів в Qualys на базі мережевого сканування

Також інвентаризацію активів можна робити використовуючи Qualys Cloud Agents – локально встановлене програмне забезпечення невеликого розміру, яке не впливає на функції операційної системи та додатків. Незважаючи на те, що агента потрібно одноразово

встановлювати на кожен актив мережі, Qualys рекомендує використовувати саме цей спосіб, бо він в режимі реального часу дає набагато більше даних, ніж одне сканування.

Мережеве сканування уразливостей. Цей процес являється стрижнем будь-якої оцінки вразливості системи, але у той же час він, як правило, потребує багато часу на обговорення. Насправді, легкою частиною процесу оцінки вразливості безпеки є виявлення тисяч або десятків тисяч вразливостей у типовій корпоративній мережі. Завдання полягає аналізі маси даних о вразливостях, знайдених в процесі сканування.

Оскільки Qualys поставляється як хмарна послуга, сканування доступних с Інтернету ресурсів може починатися одразу. Але для управління вразливостями саме локальної мережі, до неї потрібно підключити мережевий сканер, який може виступати апаратним засобом або віртуальною машиною. Сканування можна створити через хмарну платформу, як показано на рисунку 2. В цьому випадку потрібно створити профіль сканування, в якому указуються такі настройки, як тип сканування, кількість портів, автентифікація тощо. Також на пристрої з встановленим Cloud Agent автоматично буде проводитися автентифіковані сканування, які дають більш детальну інформацію об активах.

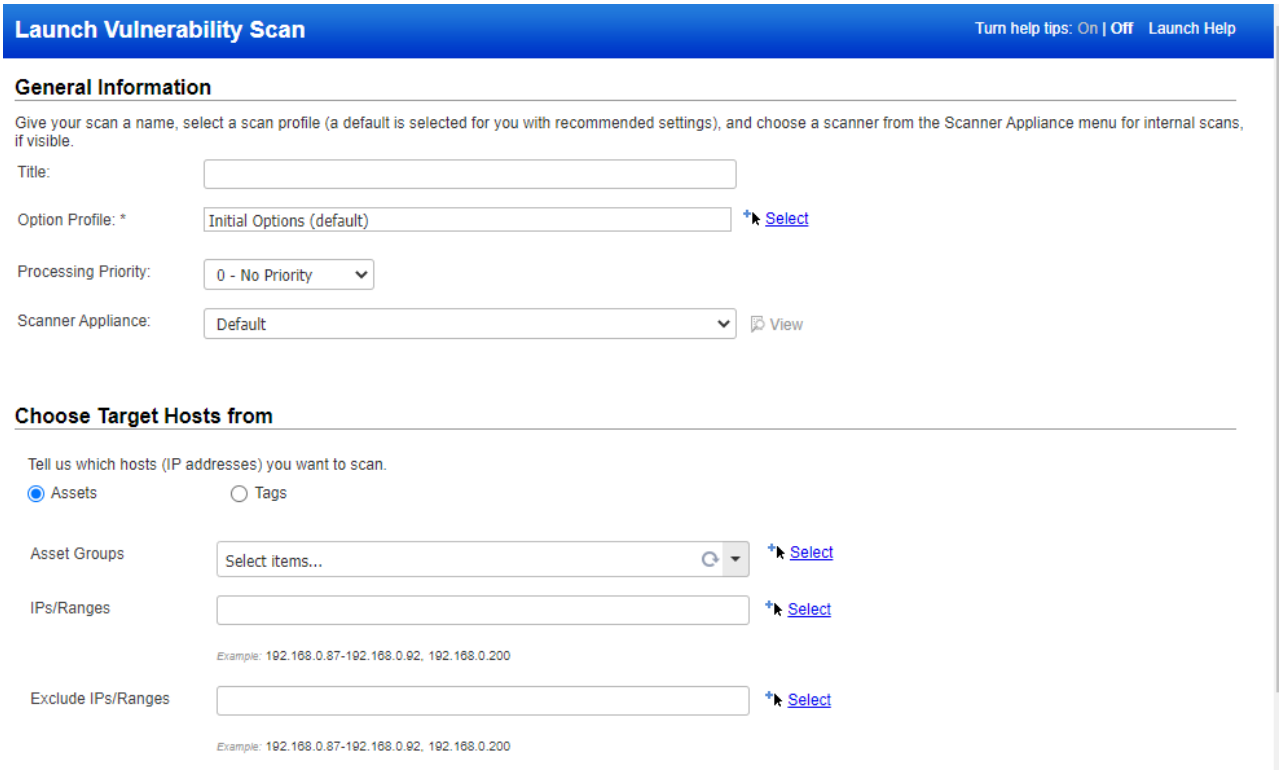

Рис. 2. Створення сканування вразливостей на платформі Qualys

Результати сканування можуть бути неповними, безрезультатними або суперечливими. Деякі налаштування можуть знадобитися, щоб знайти правильний варіант для кожного середовища. Обов'язково треба додавати в білий список IP-адреси, пов'язані зі сканером, на стороні корпоративного брандмауера. В іншому випадку він може відфільтрувати будь-які спроби підключення до різних портів, тобто можна буде побачити, що всі порти закриті і вразливості відсутні. Життєво необхідно забезпечити достовірність результатів, перш ніж аналізувати їх.

Сканування веб-додатків. Ключовим елементом всебічної оцінки вразливості безпеки є виявлення та тестування веб-додатків. Вразливості веб-додатків можуть мати десятки форм. Наприклад, у багатьох атаках використовується ін'єкція несправностей, яка використовує вразливі місця в синтаксисі та семантиці веб-додатків. Простіше кажучи, зловмисник маніпулює даними на веб-сторінці, використовуючи «Уніфікований індикатор ресурсу» (URL), щоб змусити застосувати несправність програми. Дві найпоширеніші

різновиди – це SQL ін'єкція та cross-site scripting. Розглянемо типову URL-адресу: http://example/test?op=1. Виконання експлойту введення SQL просто вимагає модифікації URL-адреси. Все, що потрібно, може бути одним непарним символом для успішного використання, наприклад, додаванням апострофа в кінці URL-адреси: http://example/test?op=1'. Успішний результат може надати зловмиснику контроль над додатком та легкий доступ до сервера, бази даних та інших внутрішніх IT-ресурсів. Цей доступ може спричинити катастрофічні результати.

Qualys Web Application Scanning забезпечується як послуга SaaS, тобто підприємство контролює її через веб-браузер. WAS бере інформацію, зібрану на етапі сканування, для створення відповідного набору тестів для виконання на веб-додатку. Ці тести визначають загальні вразливості на сайті. Поки сканер проводить ці тести, він перевіряє вміст відповідей сайту, щоб визначити наявність певної вразливості. Qualys WAS також використовує дані профілювання сканера для налаштування тестів на вразливість. Приклад інформаційної панелі Qualys Web Application Scanning зображено на рисунку 3.

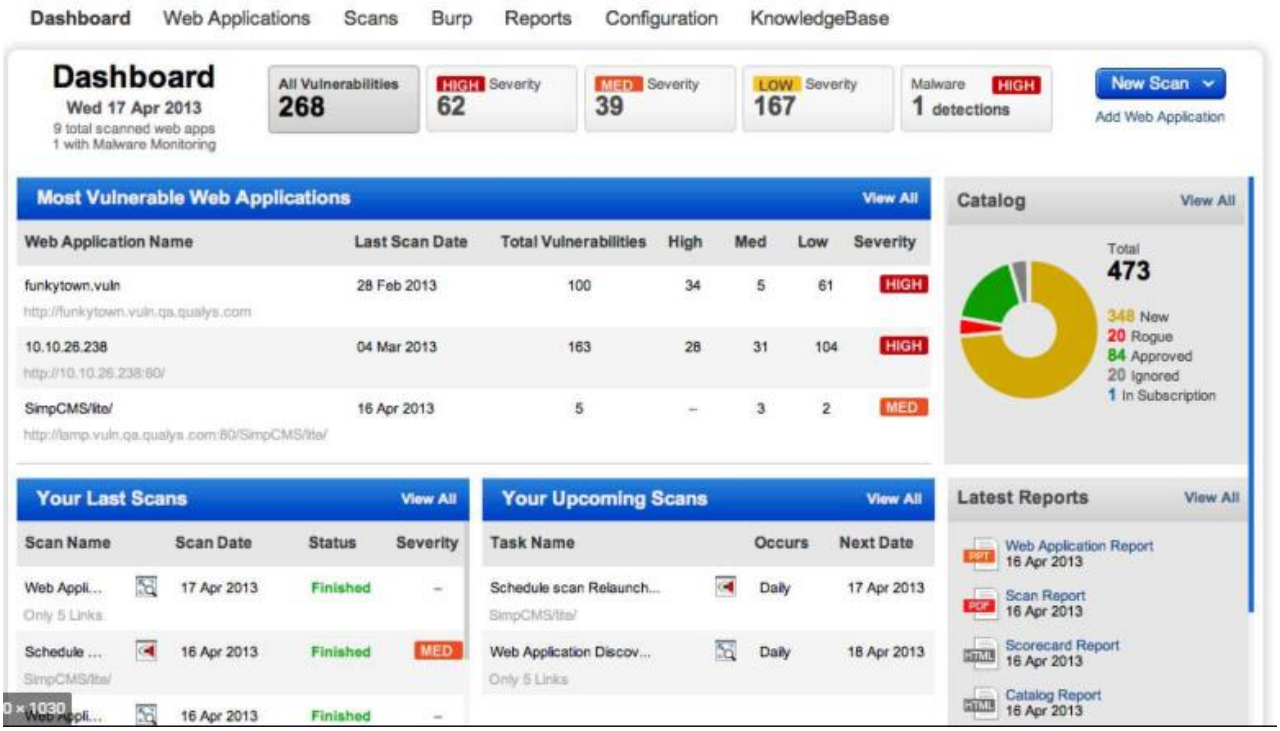

Рис. 3. Інформаційна панель Qualys Web Application Scanning

Звітність. Після завершення сканування починається фаза процесу звітування. Технологія управління вразливостями Qualys передбачає як детальну, так і зведену звітність. Приклад звіту створено після сканування Cloud Agent приведено на рисунку 4. Такі звіти особливо корисні для збору даних про високий рівень, які можуть бути представлені керівникам організації. Також о кожній вразливості в звіті можна отримати інформацію про ступінь серйозності вразливості, деталі її виявлення та кроки з її виправлення. Ці данні спрямовані на технічний персонал і надають їм інформацію щодо вирішенні цих завдань.

Qualys WAS представляє інформацію про вразливість веб-додатків із простим у користуванні інтерфейсом для стандартних браузерів. Центр полегшує роботу з багатьма веб-додатками так само, як і для одного веб-сайту. Інтерфейс забезпечує просту навігацію функціями WAS, а також інтегрує та чітко відображає результати аналізу та тестування на основі даних сканування вразливостей. Ці дані зіставляється з OWASP Top 10 2017 vulnerabilities, приклад зображено на рисунку 5. О кожній знайденій вразливості можна отримати детальний опис, а також спосіб її виправлення.

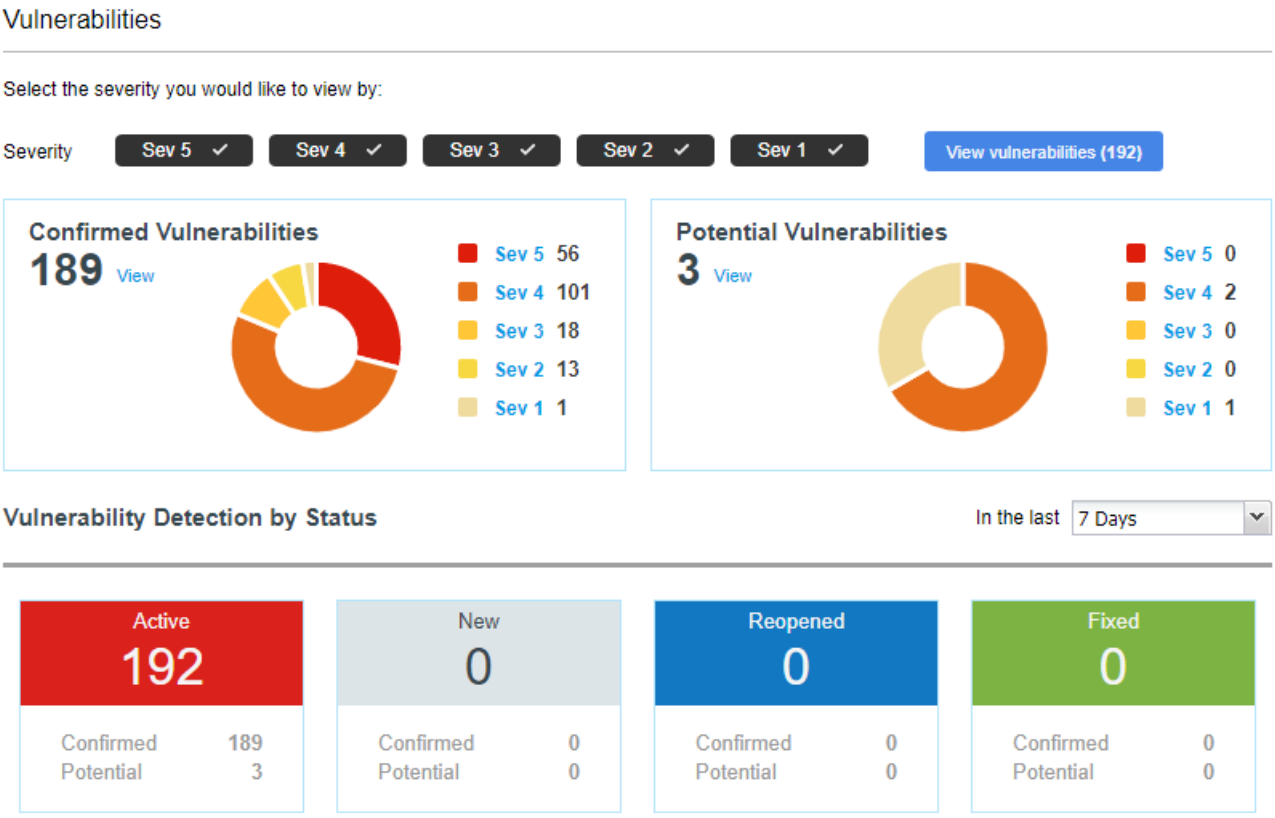

Рис. 4. Звітність Qualys Cloud Agent

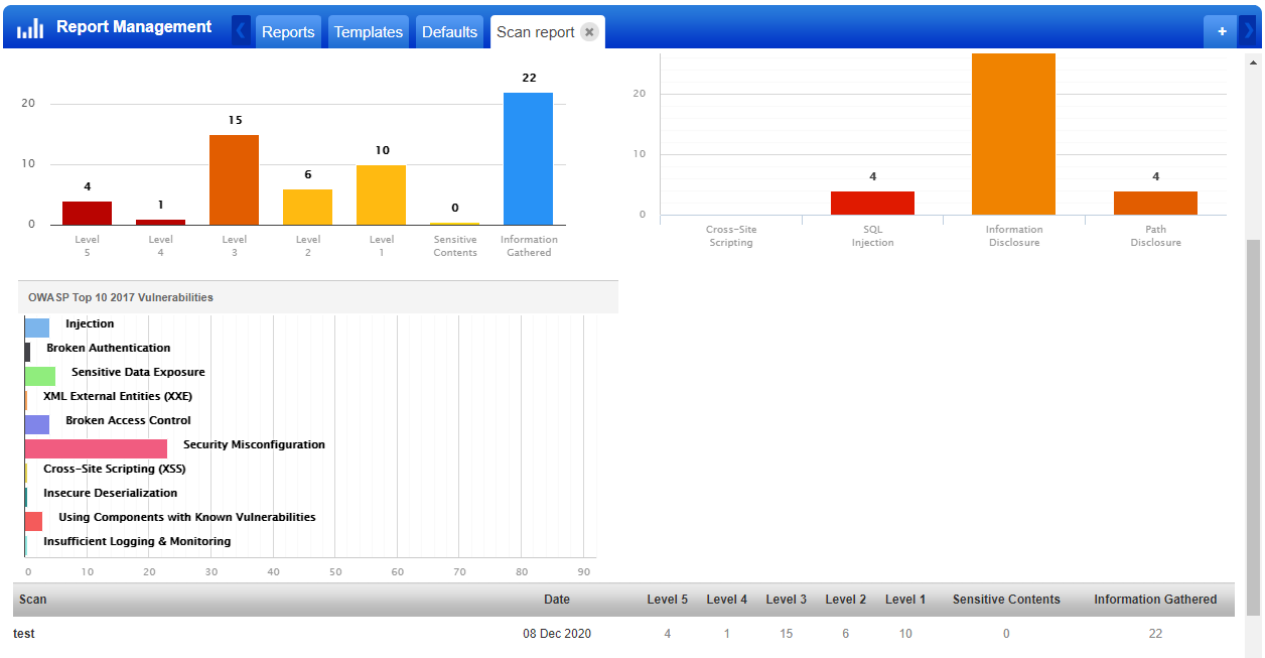

Рис. 5. Звіт сканування веб-додатку на платформі Qualys

Після проведення оцінювання вразливостей критично важливо створювати чіткі і легко зрозумілі звіти з пріоритетними завданнями щодо виправлення. Незалежно від того, який інструмент сканування вразливостей використовується, він повинен допомагати складати звіти, відзначати вразливості як виправлені або не виявленні, відстежувати вік вразливостей тощо. Перед публікацією звіту організація повинна погодити його формат. Як і у випадку з багатьма іншими критично важливими процесами безпеки, настійно рекомендується, щоб вище керівництво було повністю залучено в процес звітності та усунення вразливостей.

Виправлення уразливостей. Метою цього кроку в технології управління вразливостями є оптимізація ресурсів для виправлення та гарантування того, що всі зусилля щодо нього врівноважують ризики, пов'язані з оновленням інформаційної системи. Після усунення вразливості необхідно призначити повторне сканування, щоб перевірити, чи були проведені виправні дії. Це сканування має бути виконаним з використанням того самого сканеру вразливостей та однакових налаштувань конфігурації, що були і при початковому скануванні. Цей крок дуже важливий для запобігання неточним результатам через помилки конфігурації. Як правило, повторне сканування планується після закінчення граничного терміну здійснення виправних заходів. Для цих сканувань створюються однотипні звіти. Керівництву та власникам активів буде потрібно дізнатись, як змінився ризик після виправних дій. ІТ-відділ буде цікавитись ефективністю здійснених заходів.

Висновки

В статті проведено дослідження та аналіз проблеми забезпечення захисту корпоративних інформаційних систем, встановлена проблематика їх захисту, яка обумовлена вразливостями. Проаналізовано етапи забезпечення технології управління вразливостями. Досліджена технологія управління вразливостями на прикладі рішення Qualys. Визначено методи та засоби забезпечення управління вразливостями, які реалізовані в рішенні Qualys.

Встановлено основні функції та принципи роботи рішення з процесу управління вразливостями на базі Qualys. Qualys – це один із світових лідерів в області забезпечення процесу управління вразливостями. Оскільки ця технологія включає в себе комплекс організаційних методів, які є індивідуальними для кожного підприємства, Qualys не спроможній забезпечити її сам по собі. У той же час, Qualys являється постачальником технічних засобів, які інтегровані в єдине рішення і суттєво спрощують кожен етап циклу процесу управління вразливостями. Оскільки Qualys реалізує свої методи, як хмарну послугу, їх інтеграція в бізнес процеси підприємства буде простим. Також Qualys має засоби, які реалізуються в локальному середовищі.

Таким чином, правильна реалізація технології управління вразливостями корпоративних інформаційних систем на базі рішення Qualys має суттєво знизити ризик компрометації конференційних даних та в цілому підвищує рівень кібербезпеки підприємства.

Перелік посилань

1. 2019 Verizon Data Breach Investigations Report [Електронний ресурс]: Verizon Communications – Электрон. дан. – Нью-Йорк, США – 2019 – Режим доступа: World Wide Web. – URL: https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

2. Cost of a Data Breach Report highlights [Електронний ресурс]: IBM – Электрон. дан. – Армонк, Нью-Йорк, США – 2020 – Режим доступа: World Wide Web. – URL: https://www.ibm.com/security/data-breach

3. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach [Електронний ресурс]: Federal Trade Commission – Электрон. дан. – Вашингтон, США – 2017 – Режим доступа: World Wide Web. – URL: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

4. The 20 CIS Controls & Resources [Електронний ресурс]: Center for Internet Security – Электрон. дан. – 2020 – Режим доступа: World Wide Web. – URL: https://www.cisecurity.org/controls/cis-controls-list/

5. Josh Zelonis and Trevor Lyness. The Forrester Wave: Vulnerability Risk Management – October 17, Q4, 2019

6. Qualys Reviews in Vulnerability Assessment [Електронний ресурс]: Gartner peer insights – Электрон. дан. – Стэмфорд, Коннектикут, США – 2020 – Режим доступа: World Wide Web. – URL: https://www.gartner.com/reviews/market/vulnerability-assessment/compare/qualys

7. Vulnerability Management For Dummies / Wolfgang Kandek;. — John Wiley & Sons, Ltd, 2015. – 80 p. – ISBN: 978-1-119-13150-2.

Надійшла: 04.04.2021 Рецензент: д.т.н., професор Гайдур Г.І.