УДК 004.056.5
DOI: 10.31673/2409-7292.2020.032933

Галузін І.С.

УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ І ОЦІНЮВАННЯ ВРАЗЛИВОСТЕЙ ЯК ЗАСОБИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Розглянуто роль методів управління вразливостями і оцінювання вразливостей у забезпеченні кібербезпеки підприємства. Проаналізовані функціональні відмінності між ними. Обґрунтовано використання технології управління вразливостями, як кращої стратегії для виявлення і усунення ризиків та виявлено оптимальний спосіб її забезпечення. Розроблено рекомендації організаціям щодо досягнення максимального результату ведення процесу управління вразливостями.

Ключові слова: управління вразливостями, оцінювання вразливостей, сканування вразливостей, ризик.

Вступ

На сьогоднішньому конкурентному ринку підприємства не можуть дозволити собі втрачати час та гроші через порушення безпеки. Компанії можуть понести незмірні збитки, якщо в центрі обробки даних відбудеться перерва в роботі через мережевого хробака, вірусу, хакеру, який завдав шкоди веб-сайту або якщо буде вкрадена важлива інформація про клієнтів. Страх втрати доходів повинен спонукати організації почати вживати активних заходів щодо вразливостей їх корпоративних мереж. Тільки шляхом виявлення і усунення вразливостей в IT-середовищі організація може запобігти проникненню зловмисників в їх мережі та крадіжці інформації. Все частіше почали з’являтися в технічній літературі такі терміни, як сканування вразливостей, оцінювання вразливостей і управління вразливостями. В цій статі буде проаналізовано роль цих методів в ліквідації ризиків компрометації їх інформаційних систем.

Основна частина.

Метод оцінювання вразливостей

Оцінювання вразливостей - це процес визначення, ідентифікації, класифікації та пріоритезації вразливостей в комп'ютерних системах, додатках і мережевих інфраструктурах [1]. Оцінювання вразливостей також дає організації необхідні знання, обізнаність та відомості про ризики і дає змогу розуміти і реагувати на загрози для свого середовища. Організації будь-якого розміру або навіть окремі особи, які стикаються з підвищеним ризиком кібератак, можуть отримати користь з тієї чи іншої форми оцінки вразливостей, але великі підприємства і інші типи організацій, які піддаються постійним атакам, отримають найбільшу вигоду.

Сканування вразливостей

Існують різні способи оцінки вразливостей, але одним з найбільш поширених є використання програмного забезпечення для автоматичного сканування вразливостей. Ці інструменти використовують бази даних відомих вразливостей для виявлення потенційних недоліків у мережах, додатках, контейнерах, системах, даних, обладнанні тощо. Оскільки метод оцінювання вразливостей пов'язаний зі скануванням вразливостей, важливо розуміти, як саме воно виконується і які інструменти для цього можуть бути використаними. Сьогодні рівень технічних знань потрібний для роботи із засобом сканування вразливостей не є високим. Більшістю сканерів вразливостей можна керувати за допомогою графічного інтерфейсу, який дозволяє швидко запустити перевірку вразливостей всієї мережі за допомогою декількох дотиків миші. Кілька постачальників надають різні технічні рішення з різними варіантами розгортання. Ці варіанти включають автономні, керовані служби або навіть хмарне програмне забезпечення, як послуга (SaaS). Деякі з постачальників, що пропонують технологію сканування вразливостей: McAfee, Qualys, Rapid7, Tenable Network Security [2]. Також є кілька проектів з відкритим вихідним кодом. Рекомендується, щоб організація ретельно протестувала продукти для сканування вразливостей, перш ніж вирішити, яке рішення найкраще відповідає вимогам організації. Слід звернути увагу на той факт, що сканування однієї системи декількома продуктами з використанням їх налаштувань

за замовчуванням може дати дуже різні результати. Незалежно від того, яке рішення для сканування вразливостей вибрано, важливо правильно налаштувати сканування, щоб обмежити його кількість помилкових спрацьовувань.

Інструмент оцінки вразливості всебічно просканує всі аспекти інформаційної системи. Після завершення сканування інструмент покаже кількість потенційних вразливостей, їх ризик, а також надасть рекомендації щодо усунення. Приклад звіту після сканування вразливостей наведено на рис. 1.

Office Server Vulnerability Summary | Host Summary — Download Report
Completed: Jan 31, 2013 14:30 — Remove Vulnerability | Audit Trail

Filters No Filters Add Filter — Clear Filters

Plugin ID	Count	Severity	Name	Family
10380	1	Critical	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely
25216	1	Critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Misc.
32314	1	Critical	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely
51988	1	Critical	Rogue Shell Backdoor Detection	Backdoors
55523	1	Critical	vsftpd Smiley Face Backdoor	FTP
61708	1	Critical	VNC Server 'password' Password	Gain a shell remotely
10205	1	High	rlogin Service Detection	Service detection
10245	1	High	rsh Service Detection	Service detection
10481	1	High	MySQL Unpassworded Account Check	Databases
33447	1	High	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS
42411	1	High	Microsoft Windows SMB Shares Unprivileged Access	Windows
10056	1	Medium	/doc Directory Browsable	CGI abuses
10079	1	Medium	Anonymous FTP Enabled	FTP
10203	1	Medium	rexecd Service Detection	Service detection
11213	1	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
12217	1	Medium	DNS Server Cache Snooping Remote Information Disclosure	DNS
15901	1	Medium	SSL Certificate Expiry	General
20007	1	Medium	SSL Version 2 (v2) Protocol Detection	Service detection
26928	1	Medium	SSL Weak Cipher Suites Supported	General
31705	1	Medium	SSL Anonymous Cipher Suites Supported	Service detection
42256	1	Medium	NFS Shares World Readable	RPC

Рис. 1. Приклад звіту після скануванням інструментом від Tenable Network Security

Оцінювання вразливостей - це не просто сканування, це разовий проект з певною датою початку і закінчення. Зазвичай зовнішній консультант з інформаційної безпеки перевірить корпоративну середу і визначить потенційні вразливості в докладному звіті. У ньому не тільки перераховуються виявлені вразливості, але і даються практичні рекомендації щодо їх усуненню. Після підготовки остаточного аналізу процес оцінювання вразливостей закінчується.

Технологія управління вразливостями

На відміну від зазвичай разового проекту оцінювання вразливостей, технологія управління вразливостями відноситься до безперервного комплексного процесу, націленого на комплексне і безперервне управління вразливостями організації. Зібрано кілька ключових характеристик і елементів стандартного підходу до управління вразливостями.

Безперервний процес

На відміну від оцінювання вразливостей, комплексна програма управління вразливостями не має певної дати початку і закінчення та являє собою безперервний процес, який в ідеалі допомагає організаціям краще управляти своїми ризиками в довгостроковій перспективі.

Рекомендований метод.

Згідно 20 Critical Security Controls, випущеним Center for Internet Security [3], одним з п'яти найбільш важливих елементів управління для усунення переважної більшості вразливостей організації є «постійне оцінювання вразливостей і їх усунення». У цьому сенсі впровадження комплексного процесу управління вразливостями є основою ефективної програми безпеки для посилення захисту організації.

Багатоскладовий метод

Технологія управління вразливостями може включати в собі безліч різних проектів, включаючи метод оцінювання вразливостей, який є важливою, але не єдиною частиною

комплексної стратегії. За даними інституту SANS [4], ефективна програма управління вразливостями включає як мінімум шість різних етапів, які повинні повторюватися на постійній основі:

Інвентаризація активів

Одним з перших кроків, які необхідно зробити в програмі управління вразливостями, є інвентаризація активів. 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.

Відповідно до передової практиці інвентаризації активів, управління активами має перебувати в руках єдиного органу, який проводить консультації з діючими мережевими картами, виконує відповідне сканування у всіх локальних мережах, регулярно перевіряє інвентаризацію активів і фіксує їх зміни. Функція централізованої інвентаризації активів може допомогти отримати ясність про інвентаризацію активів організації і зміцнити її стан безпеки.

Управління інформацією

Після того, як організація визначила всі свої активи і продовжує регулярно ними управляти, важливим кроком управління вразливостями стає управління інформацією. Інформація, що відноситься до безпеки, постійно змінюється, і багатьом організаціям складно тримати своїх співробітників в курсі актуальних концепцій безпеки, наприклад, мережі, програмування, криміналістики або моніторингу. Найчастіше складні технічні концепції безпеки не передаються, або не доводяться до відома всієї організації, в результаті чого співробітники залишаються неінформованими про те, як дотримуватися передових рекомендацій забезпечення безпеки.

Ефективна методологія управління вразливостями включає спеціальну групу реагування на інциденти комп'ютерної безпеки (CSIRT). CSIRT відповідає за публікацію рекомендацій з безпеки, проводить регулярні конференц-дзвінки для обговорення шкідливої активності і останніх атак нульового дня, спрощує і поширює попередження щодо концепцій кібербезпеки і розробляє зрозумілі і ефективні інструкції з реагування на інциденти для всіх співробітників. Таким чином, співробітники зможуть реагувати на потенційні індикатори компрометації відповідно до кращих практик, рекомендованими командою CSIRT.

Оцінка ризиків

Ще одна важлива область ефективної стратегії управління вразливостями - це належна оцінка ризиків та управління ними. В більшості організацій відсутня належна документація, щодо управління ризиками, а окремі відділи не обмінюється інформацією о своїх відповідних критичних активах і пов'язаної з ними цінності. Управління змінами не практикується або відбувається тільки в дуже обмеженому масштабі.

Оцінка ризиків має вирішальне значення для розуміння різних загроз вашим IT-систем, визначення рівня ризику, якому ці системи піддаються, і для рекомендацій їх відповідного рівня захисту. Ретельна оцінка ризиків допоможе організаціям провести їх формальну перевірку, дозволить власникам активів прийняти допустимі рівні ризиків, якщо їх усунення нерентабельне, затвердити високі ризики на рівні керівництва організації і запланувати їх перевірки на регулярній основі. Якщо в організації немає спеціального програмного забезпечення по управлінню ризиками, то контрольні списки або електронні таблиці Excel допоможуть спростити ситуацію. Також знадобяться надійні методи документування політик і процесів безпеки.

Оцінювання вразливостей

Як згадувалося раніше, метод оцінювання вразливостей сам по собі є важливим елементом структури управління вразливостями і вважається першим кроком на шляху до підвищення вашої IT-безпеки. Багато організацій борються з величезною кількістю невідомих активів, погано налаштованими мережевими пристроями, сильно сегментованими

середовищами, несумісними інструментами або просто занадто великим обсягом інформації для аналізу і обробки. Оцінювання вразливостей має безліч переваг і дозволить виявити ключові інформаційні активи вашої організації, визначити уразливості, які загрожують безпеці цих активів, надати рекомендації щодо посилення вашої безпеки і допомогти знизити ризики, тим самим дозволяючи вам більш ефективно зосередити свої IT-ресурси. .

Сканування вразливостей з перевіркою достовірності дозволить провести повну інвентаризацію всього програмного забезпечення і його точних версій, а також дасть можливість перевіряти базові конфігурації безпеки і виявляти уразливості. О таких перевірках слід оголошувати, щоб можна було відзначити несанкціоновані сканування і полегшити відстеження змін мережі і активів. Процеси сканування повинні бути задокументовані і перевірені.

Звітність та виправлення

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 уразливості як виправлені або не виявленні, відстежувати вік вразливостей тощо. Перед публікацією звіту організація повинна погодити формат звіту. 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.

Планування протидій

Регулярно організації отримують найсвіжіші рекомендації з кібербезпеки і їм необхідно виділити команду, яка розбирається у всій цій інформації. У багатьох випадках підприємствам не вистачає ресурсів, необхідних для негайного впровадження критичних змін, у них немає чітко визначених процесів для внесення цих змін або вони просто не знають, які активи у них є, які потенційно можуть бути уразливі і становити ризик для організації. в цілому.

В рамках ефективного процесу планування реагування наявність точної та актуальної інвентаризації активів є базовим критерієм для команди CSIRT для ефективного і дієвого реагування на уразливості. У разі нової уразливості або загрози команда CSIRT несе відповідальність за негайне інформування всієї організації і роботу з програмним забезпеченням для управління виправленнями. Для досягнення максимальних результатів це програмне забезпечення повинно бути інтегровано як з базою даних вразливостей, так і з системою інвентаризації активів.

Після того, як ці шість найважливіших кроків будуть виконані, організаціям рекомендується продовжувати повторювати їх на регулярній основі. На відміну від сканування або оцінювання вразливостей, ефективність управління вразливостями полягає в його безперервності.

Висновок

Кількість вразливостей і створених до них експлойтів зростає з кожним днем. Організації повинні діяти негайно і ефективно, щоб захистити себе. Їм потрібні ефективні способи усунення існуючих ризиків, пов'язаних з кібербезпекою. Ми розглянули метод оцінювання вразливостей, який завдяки сучасним сканерам вразливостей, графічно показує інформацію про ризики й способи їх усунення. Проте, отримані результати необхідно проаналізувати, зіставити до поточних потреб організації і придумати рентабельні контрзаходи для ліквідації ризиків. Динаміка розвитку останніх, в слідстві поширення вразливостей програмного забезпечення, вимагає регулярного повторення цих дій. Тому в концепції забезпечення більш досконалого кіберзахисту підприємства, метод оцінювання вразливостей може розглядатися тільки як складова частина технології управління вразливостями. Оскільки ця технологія включає в себе не тільки технічні, але і організаційні способи ліквідації ризиків, то її можна визначити як найбільш кращий спосіб допомогти організаціям скоротити ресурси, що витрачаються на боротьбу з вразливостями у своєму середовищі.

Перелік посилань

1. Risk management strategies. Vulnerability Assessment (Vulnerability Analysis) [Електронний ресурс] // - Режим доступу: https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis/ (10.06.2020)

2. SANS Institute. Implementing a vulnerability management process [Електронний ресурс] // - Режим доступу: https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis/ (10.06.2020)

3. Center for Internet Security. 20 Critical Security Controls [Електронний ресурс] // - Режим доступу: https://www.cisecurity.org/controls/cis-controls-list// (10.06.2020)

4. SANS Institute. Vulnerability Management: Tools, Challenges and Best Practices [Електронний ресурс] // - Режим доступу: https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis/ (10.06.2020)

Надійшла: 27.06.2020 Рецензент: д.т.н., професор Гайдур Г.І.