УДК 004.056.52 **DOI:10.30837/rt.2020.4.203.11**

В.О. ПОДДУБНИЙ, О.В. СЄВЄРІНОВ, канд. техн. наук

МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ ФОРМАЛІЗОВАНОГО ОПИСУ

Вступ

Захист інформації в інформаційно-телекомунікаційних системах (далі – ІТС) під час її функціонування потребує не тільки дотримання політики безпеки, здійснення організаційних заходів чи технічного обслуговування засобів захисту, але й ефективного менеджменту, моніторингу, контролю та оцінки ризиків інформаційної безпеки (далі – ІБ). Однією із складових ефективного менеджменту ІБ в ІТС є правильне реагування на вразливості. Адже жодний розробник не може гарантувати, що в його продукті відсутні вразливості, які в свою чергу можуть призвести до негативних наслідків (від сповільнення роботи продукту до його ураження зловмисником та взяття під адміністративний контроль). Для покращення роботи ІТС необхідно відповідним чином здійснювати менеджмент вразливостей в системі, який включає систему оцінки ризиків та прийняття рішень. Тому проблема оцінки ризиків при виявленні вразливостей та правильного реагування є досить актуальною та потребує детального дослідження.

Проблеми, що виникають під час процесу керування вразливостями

Якщо розбирати основні етапи керування вразливостями в ІТС, то це будуть наступні дії [1]:

– підготовка;
– сканування на наявність вразливостей;
– визначення дій щодо виправлення;
– здійснення виправлення;
– повторне сканування.

Схематично ці етапи зображено на рис. 1.

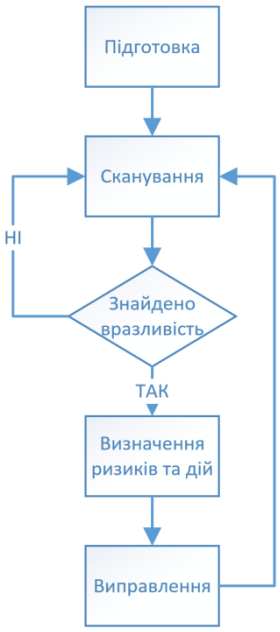

Рис. 1. Схема менеджменту вразливостями

Якщо сканування можливо автоматизувати (за допомогою спеціального програмного забезпечення), то етап визначення та прийняття дій майже цілком залежить від адміністратора

безпеки та аудиту. Адміністратор повинен здійснити оцінку ризику та відреагувати відповідним чином (оновлення, відкат, мінімізація роботи процесу, здійснення налаштувань тощо). Незважаючи на наявність систем оцінки вразливостей (таких як CVSS), які надають якісну оцінку серйозності певної вразливості, вплив і поводження окремої вразливості різний для кожної інформаційної системи, так як такі системи оцінки не враховують безліч факторів (структуру і склад інформаційної системи, критичність ресурсів, взаємозв'язки процесів). Тобто вся система стає залежною виключно від досвіду та знань адміністратора. Ця проблема становиться більш гострою в складних системах, з великою кількістю компонентів, які взаємодіють між собою, адже в такій системі складно прослідкувати вплив вразливості. Під час зміни персоналу ІТС стає найбільш вразливою, оскільки новому адміністратору потрібний час для опанування принципів роботи ІТС.

В даний час існує низка міжнародних стандартів серії ISO/IEC 27035 [2] (який є гармонізованим стандартом в Україні [3]), які можуть допомогти в прийнятті рішень. Проте серія ISO/IEC 27035 є загальним зводом практик, а не конкретною інструкцією щодо визначень ризиків чи дій адміністратору. Міжнародний стандарт ISO/IEC 27005 [4] забезпечує рекомендації для управління ризиків ІБ в організації, особливо підтримуючи вимоги СУІБ (ISMS) згідно ISO/IEC 27001 [5]. Однак цей міжнародний стандарт не забезпечує певної методології для управління ризиків ІБ[6].

Тому на даний момент необхідна така система оцінювання ризиків, яка:

– відслідковуватиме вплив вразливості на компоненти системи;

– забезпечуватиме відтворюваність результатів;

– буде ефективною для складних систем;

– повинна бути зрозумілою та гнучкою у використанні.

Така система не виключить вплив адміністратора безпеки та аудиту, проте допоможе йому в прийнятті рішень, оцінці ризиків, зменшить вірогідність помилок, допоможе новому персоналу під час вибору рішень.

Неформалізований та формалізований опис ІТС

Під час опису інформаційної системи та системи захисту інформації зазвичай використовують неформалізований опис, тому, на перший погляд, створювана система оцінювання та прийняття рішень повинна також бути неформалізованою, але це не найкращий варіант, адже неформалізований опис створює безліч проблем, а саме: складність розуміння системи новим персоналом, громіздкість опису систем, відсутність єдиного структурованого опису, погіршення опису взаємозв’язків процесів, знецінення важливої інформації, погану гнучкість.

Відсутність структурованого опису походить від того, що при неформалізованому описі системи розробник не має чітких вимог до структури та форми опису системи, тому зазвичай розробники ІТС під час опису керуються власними нормами або узгоджують їх з клієнтом. Тому опис різних ІТС може відрізнятися якщо вони були створені різними розробниками, навіть якщо ці системи створені однією фірмою, то вони можуть відрізнятися в залежності від типу ІТС, замовника, працівників, що займалися розробкою.

Громіздкість опису системи походить від того, що вся інформація при неформалізованому описі зазвичай подається у вигляді тексту та відсутності структурованого опису. Чим більша система, чим більше процесів та об’єктів, тим більший опис з’являється на виході. Ситуація погіршується, якщо описувана система має обширні або специфічні зв’язки між об’єктами.

Гнучкість опису системи проявляється при її модернізації. Під час модернізації неформалізованого опису необхідне редагування безлічі частин опису, які можуть бути пов’язані або залежати одна від одної. Тому внесення навіть мінімальних правок в систему призводить до перегляду всього опису в цілому, не кажучи вже про додавання або виключення компонентів системи.

Під час такого опису погіршується відображення взаємозв'язків процесів, адже чим довше та складніше дерево об'єктів або процесів, тим складніше його описати та тим більше буде опис системи. Також під час такого опису неможливо чітко дати оцінку впливу вразливості в одному об'єкті ІТС на інший, оскільки не існує метрик, формул та правил взаємодії. Ці правила встановлюються емпіричним методом на базі знань адміністратора.

З цих проблем виникає складність розуміння новим персоналом специфіки роботи системи. Такому персоналу слід обробити безліч інформації в текстовому представленні, яка структурно може відрізнятися від тієї з якою персонал працював раніше.

Під час такої обробки складно виділяти та концентрувати увагу, відслідковувати взаємозв'язки процесів та об'єктів, структурно та логічно класифікувати її, тому можливе погіршення обробки інформації та її знецінення.

Ці проблеми переходять на створювану систему оцінки вразливостей та посилюються там. Така система буде нечіткою, вузькоспеціалізованою, не враховуватиме всіх взаємозв'язків процесів та матиме вигляд зводу практик (аналогічно ISO/IEC 27035). Такі практики не надають методів обчислення ризиків чи впливу вразливості на різні компоненти ІТС. Весь тягар оцінки впливу вразливостей, оцінки ризику, прийняття рішень, покладено на адміністратора безпеки. При різних адміністраторах одна і та ж ситуація може трактуватися порізному, відповідно і рішення будуть прийняті різні в залежності від досвіду, темпераменту адміністратора. В додаток до цих проблем неформалізований опис не може гарантувати рівень гарантій вище ніж Г-2 [7]. Для рівнів Г-3, Г-4, Г-5 стиль опису ІТС повинен бути частково-формалізований, для Г-6 та Г-3 – формалізований.

На відміну від неформалізованого опису системи формалізований має чітку структуру та форму опису, відображає взаємозв'язки процесів, є гнучким та універсальним. В такій системі вплив вразливості легко відслідкувати від точки контакту до всіх об'єктів інформаційної системи. Формалізація дає змогу виявити загальну структуру системи, сформулювати на цій основі загальні закони і правила, за якими відбувається визначення впливу вразливостей на ІТС. Така система зводить до мінімуму вплив адміністратора безпеки, покладаючи оцінку впливу та ризиків на чіткі та закріплені методики, забезпечуючи однозначність та відтворюваність результатів. Тому розроблена система оцінювання ризиків повинна бути формалізованою та побудованою над формалізованим описом ІТС.

Суміщення формалізованого опису та менеджменту вразливостями

Варіантом формалізованого опису ІТС може бути опис послуг безпеки в ІТС. Під час такого опису об'єкти та процеси інформаційної системи представляються в описі зі сторони послуг безпеки, які вони надають або обробляють. Ці послуги передаються від об'єкта до об'єкта, посилюються або взаємодіють з ними. Під час такої реалізації, вразливості будуть розцінюватися як небезпека для конкретної послуги безпеки.

Суміщення формалізованого опису та менеджменту вразливостей допоможе виявляти слабкі місця в ІТС, відслідковувати вплив окремої вразливості на компоненти, масштабувати вразливості, відслідковувати їх взаємозв'язок. При додаванні якісного оцінювання вразливостей можливе створення методик та інструкцій щодо оцінки ризиків. Такі методики можуть надати числову оцінку загрози як системи в цілому, її окремим компонентам, а оцінка ризиків допоможе адміністратору в виборі дій. Так як значення ризику мають числове представлення, то можливе створення чітких інструкцій щодо дій адміністратору. Також така система буде досить гнучкою і універсальною, адже будуватиметься над структурованим описом системи.

Якісне оцінювання вразливостей

Для якісного оцінювання впливу окремої вразливості на конкретний об'єкт доцільно використовувати системи оцінки вразливостей. Однією з таких систем є Common Vulnerability Scoring System (CVSS). CVSS фіксує основні технічні характеристики програмних, технічних та програмно-технічних вразливостей. Її результати включають числові показники, що вказують на серйозність вразливості відносно інших вразливостей.

CVSS складається з трьох основних метричних груп, це: базова (Base), часова (Temporal), та метрика середовища (Environmental)

Базовий показник відображає ступені якості вразливості відповідно до її внутрішніх характеристик, які є постійними в часі і передбачає найгірший вплив у різних розгорнутих середовищах (її вплив на конфіденційність, доступність та цілісність).

Часові метрики регулюють Базову групу вразливості на основі факторів, які змінюються з часом, наприклад наявності експлойтів, які використовують дану вразливість.

Показники середовища змінюють базові та часові метрики для конкретного обчислювального середовища. Вони розглядають такі фактори, як наявність пом'якшення наслідків у цьому середовищі.

Базові оцінки, зазвичай, виробляються організацією, що підтримує продукт з вразливістю, або третьою стороною від її імені. Базові метрики не змінюються з часом і є загальними для всіх середовищ

Споживачі CVSS повинні доповнити базовий показник, тимчасовими та показниками середовища, характерними для використання вразливого продукту, щоб створити точнішу оцінку для їх середовища.

Споживачі можуть використовувати інформацію CVSS як вклад у процес управління організаційною вразливістю, який також враховує фактори, які не є частиною CVSS, щоб класифікувати загрози для їх технологічної інфраструктури та приймати обґрунтовані рішення щодо виправлення.

Такими факторами можуть бути: кількість клієнтів на товарній лінійці, грошові втрати через порушення, загроза життю чи майну, або громадські настрої щодо вразливих місць. Вони виходять за рамки CVSS.

До переваг CVSS можна віднести стандартизовану методологію оцінювання вразливості для постачальників та платформ. Це відкрита структура, що забезпечує прозорість індивідуальних характеристик та методології, яка використовується для отримання оцінки [8].

CVSS є досить розповсюдженою системою, тому існує безліч баз даних, які надають доступ до оцінок вразливостей, які постійно оновлюються, таким чином, вона якнайкраще підходить для якісного оцінювання вразливостей. Однією із таких баз є National Vulnerability Database (NVD) інформаційна база даних національного органу стандартизації США, Національного інституту стандартів і технології [9]. Така база надає доступ до опису всіх виявлених вразливостей, включно з оцінкою CVSS (рис. 2).

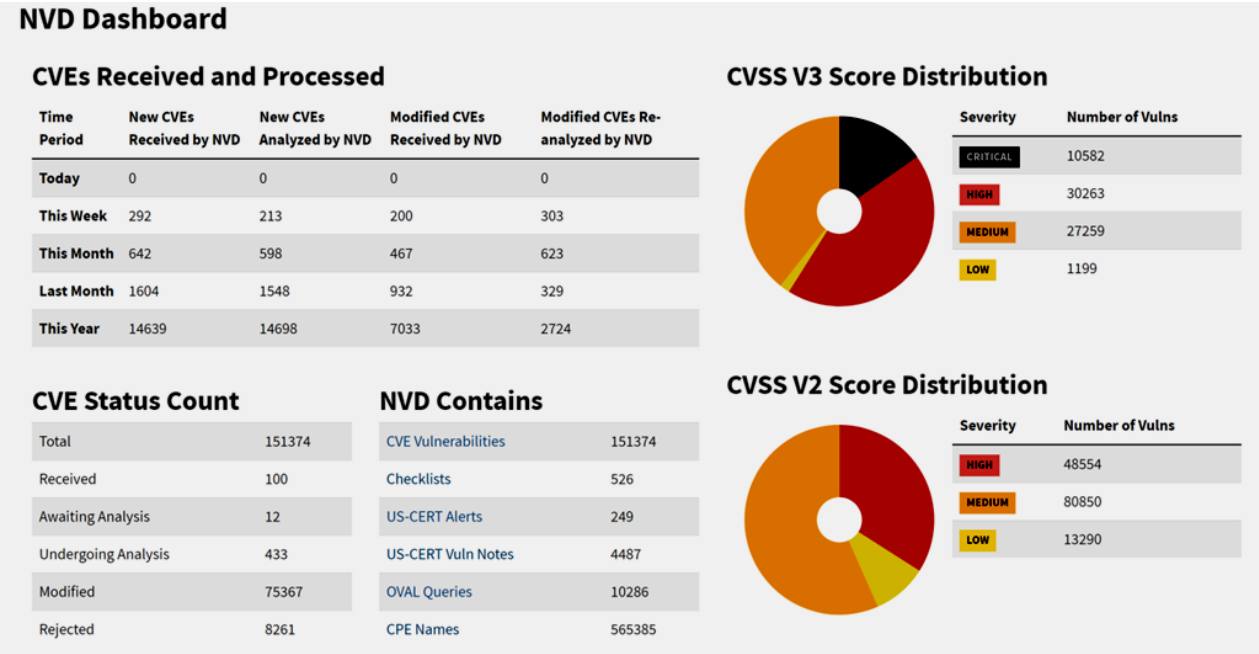

Рис. 2. Загальна інформація з бази даних NVD

Висновок

Отже, для розроблення ефективної системи керування вразливостей необхідно використовувати формалізований опис системи та систему оцінки вразливостей, на базі яких можливо формування методик, інструкцій та правил оцінки ризику. Ця система повинна бути побудована на базі формалізованого опису ІТС, так як такий опис має цілу низку переваг. Як варіантом це може бути опис послуг безпеки в ІТС. Така система буде відповідати всім сучасним вимогам, буде гнучкою, однозначною, простішою у використанні, дозволить відслідковувати вплив вразливості на всі компоненти ІТС. Також для неї легко створювати методики оцінювання ризиків для всієї системи в цілому, такі методики можуть бути модифіковані для більш точного налаштування та будуть являтися чіткими інструкціями щодо дій адміністратору. Додатковою перевагою такої системи є можливість автоматизації процесів оцінки та прийняття рішень (можливість створення ПЗ, яке на вході матиме опис системи та базу вразливостей, а на виході – оцінку ризику для кожного компоненту та процесу ІТС). Також така система може бути частиною "Матриці СУІБ" та допомогти при модернізації системи захисту інформації [10].

Список літератури:

1. Tom Palmaers, Dennis Distler, Implementing a Vulnerability Management Process // SANS Institute Information Security Reading Room, 2013. 24 с.
2. ISO/IEC 27035:2016. Information technology – Security techniques – Information security incident management, 2016. (Міжнародний стандарт)
3. Про прийняття національних стандартів, про прийняття поправок до національних стандартів: затв. Національним Органом Стандартизації від 10 грудня 2018 р. №470
4 ISO/IEC 27005 Information technology – Security techniques – Information security risk management, 2018. (Міжнародний стандарт)
5 ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, 2013. (Міжнародний стандарт)
6. Сєвєрінов О. В., Черниш В. І., Молчанова М. Є. Управління інформаційною безпекою згідно міжнародних стандартів //Системи управління, навігації та зв'язку. Вип. 2011. Т. 4. С. 250-253.
7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. 61с.
8. Common Vulnerability Scoring System version 3.1: Specification Document [Електронний ресурс] Режим доступу: https://www.first.org/cvss/specification-document
9. National Vulnerability Database [Електронний ресурс] Режим доступу: https://nvd.nist.gov
10. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України. 2014. №. 2. С. 133-138.

Надійшла до редколегії 03.11.2020

Відомості про авторів:

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії, Харківський національний університет радіоелектроніки, Україна; e-mail: oleksandr.sievierinov@nure.ua, ORCID: https://orcid.org/0000-0002-6327-6405

Поддубний Вадим Олександрович –магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: vadym.poddubnyi@nure.ua