DOI: https://doi.org/10.30525/978-9934-26-191-6-29

Ellana Molchanova
Ph.D. in Economics, Associate Professor
Kyiv National University of Trade and Economics
Oleh Ilarionov
Ph.D. in Engineering Sciences
Taras Shevchenko National University of Kyiv

ASSESSMENT OF THE COMPANY'S SECURITY SYSTEM FRAGILITY

Summary

The research shows how one of the crisis teams should determine the cause of an undesirable incident (vulnerabilities may be errors in software design and development (firmware), improper change of modes of operation of devices and programs, or failures in their work), assess vulnerabilities in information technology. Emphasis placed on assessing security vulnerabilities, which will allow companies to investigate and address vulnerabilities before they become threats. Types of cyber threats, methodology of their analysis analyzed and methods of vulnerability assessment described. It is determined that the main factor influencing the systematic monitoring and improvement of the evaluation methodology is the rapid change of technologies. The primary task of crisis teams is to identify vulnerabilities in the system that could lead to security breaches or other negative consequences if used. The vulnerability assessment examines potential threats, system vulnerabilities, and impacts to identify key vulnerabilities that need to be addresse. Identified key compromise indicators (IoCs) that indicate that an attack has occurred and can help you understand the type of attack and its source. An algorithm for detecting threats and complex solutions for their analysis proposed. The holistic vision of vulnerability assessment presented, which is demonstrated by the example of

the SmartSheet platform. The main steps in vulnerability assessment are as follows: threat assessment, vulnerability assessment, assessment of the probability of impact on a particular situation, development of a recommendation, reassessment or rethinking of threats.

Вступ

У період стрімкого розвитку інформаційних технологій та діджиталізації процесів забезпечення діяльності компанії виникають нові види ризиків та загроз. У розвинутих економіках існує практика формування антикризових кризових команд на першому етапі свого розвитку. Перш ніж будуть сформовані команди, кожному відділу доручається проаналізувати та сформувати перелік можливих ризиків та загроз. Систематизація визначених ризиків та загроз дасть змогу поділити їх на першочергові та другорядні. Дана класифікація має суб'єктивний характер, але визначає певні слабкі боки в діяльності компанії, які слід нівелювати. Виокремивши основні напрями, формуються антикризові команди.

Незалежно від діяльності компанії завжди в пріоритеті буде захист інформації. Даний вид загроз може виникнути як інцидент, який може завдати шкоди системі або організації [1]. Поняття інциденту було запозичено з моделі системи керування інцидентами [2]. Модель системи командного управління інцидентами унікальна тим, що зародилася в реальному світі, а потім була формалізована як модель. Командування інцидентами розпочалося в 1970-х роках як зразок для каліфорнійських агентств для боротьби з лісовими пожежами. Система командування подіями поділяє роботу на п'ять широких сфер, включаючи операції та матеріально-технічне забезпечення, а також ієрархію ролей та відповідальності ключових гравців, що забезпечує чіткий ланцюг командування та зв'язку. Кожна пожежна служба або сайт компанії повторюють структуру, тому команди автоматично знають своїх колег та діляться загальною інформацією. Тому координація та спільна робота стають відносно простими, а команди витрачають менше часу на організацію реакції та більше часу на реальні дії. Модель системи керування інцидентами корисна, оскільки вона пропонує основу для уніфікованого управління кризою, добре масштабується, ефективно використовує ресурси та полегшує спілкування між людьми з різних відділів чи організацій.

Сьогодні ця модель інтегрована до класичної моделі безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга – модель PDCA (плануй – Plan, виконуй – Do, перевіряй – Check, дій – Act) і виступає як основа функціонування всіх процесів системи управління інформаційною безпекою [3].

Застосування будь-якої моделі передбачає систематичний огляд слабких місць в інформаційній системі безпеки та формує процес виявлення вразливостей та загроз у системі.

Розділ 1. Огляд слабких місць в інформаційній системі безпеки

Після виявлення вразливостей та загроз у компанії формуються відповідні команди. У нашому випадку – це команда, яка має виявити причину небажаного інциденту (виникнення вразливостей може бути через помилки під час проєктування та в період розроблення програмного (програмно-апаратного) забезпечення, неправомірну зміну режимів роботи пристроїв і програм або збої в їх роботі), оцінити вразливість в інформаційних технологіях [4].

Приклади загроз, які можна запобігти за допомогою оцінки вразливості, включають:

1. SQL-ін’єкції, XSS та інші атаки з використанням ін’єкцій коду;
2. ескалація привілеїв через несправні механізми аутентифікації.

Приклади систем, для яких проводяться оцінки вразливості:

– системи інформаційних технологій;
– системи енергопостачання;
– системи водопостачання;
– транспортні системи та системи зв’язку.

Такі оцінки можуть проводитися від імені цілої низки різних організацій – від малих підприємств до великих регіональних інфраструктур. Уразливість із погляду боротьби зі стихійними лихами означає оцінку загроз, що виходять від потенційних небезпек для населення та інфраструктури. Вона може проводитися у політичній, соціальній, економічній або екологічній сферах.

Оцінка вразливості має багато спільного з оцінкою ризику. Оцінки зазвичай виконуються відповідно до таких кроків:

1) каталогізація активів і можливостей (ресурсів) у системі;
2) присвоєння цим ресурсам піддається кількісній оцінці цінності (або принаймні порядку ранжирування) і важливості;
3) виявлення вразливостей або потенційних загроз для кожного ресурсу;
4) пом’якшення або усунення найбільш серйозних уразливостей для найбільш цінних ресурсів: GSA Schedule 70, яка містить чотири основні категорії спеціальних номерів позицій (SIN), у тому числі: 132-45 A «Тестування на проникнення»; 132-45 B «Служби редагування на інциденти»; 132-45 C «Оцінка ризиків та вразливості» [5].

GSA (також відома як адміністрація загального обслуговування) стандартизувала сервіс «оцінки ризиків і вразливостей (RVA)» як попередньо перевірену службу підтримки з метою швидкого проведення оцінки загроз і вразливостей, визначення відхилення від прийнятних конфігурацій корпоративної або місцевої політики, оцінювання рівня ризику, розроблення і/або рекомендацій відповідних заходів щодо

пом’якшення наслідків в оперативних і неоперативних ситуаціях. Ця стандартизована послуга пропонує попередньо перевірені допоміжні послуги: карту мережі, сканування вразливостей, оцінку фітингу, бездротову оцінку, оцінку вебдодатків, оцінку безпеки операційної системи (OSSA), оцінку бази даних, тестування на проникнення тощо [5].

Ці послуги зазвичай називаються високоадаптивними службами кібербезпеки (HACS) і перераховані на вебсайті US GSA Advantage [5]. Послуга GSA призначена для поліпшення швидкого замовлення та розгортання послуг, скорочення дублювання державних контрактів, а також для захисту та підтримки інфраструктури більш своєчасним та ефективним чином.

132-45 С «Оцінка ризиків і вразливостей» виявляє, оцінює і визначає пріоритетні ризики і вразливості в системі. Під час оцінки ризику виявляються фактори, а також імовірність того, що ці фактори призведуть до реальних загроз.

Існує кілька типів оцінок вразливості. До них відносяться:

1. Оцінка хоста – оцінка критичних серверів, які можуть бути уразливі для атак, якщо не будуть належним чином протестовані або не будуть згенеровані з тестованого образу машини.

2. Оцінка мереж і бездротових мереж – оцінка політики та практики запобігання несанкціонованому доступу до приватних або публічних мереж і мережевих ресурсів.

3. Оцінка баз даних – оцінка баз даних або систем великих даних на предмет вразливостей і неправильної конфігурації, виявлення шахрайських баз даних або небезпечних середовищ розроблення/тестування, а також класифікація конфіденційних даних по всій інфраструктурі організації.

4. Сканування додатків – виявлення вразливостей безпеки у вебдодатках та їх вихідному коді шляхом автоматизованого сканування на інтерфейсі або статичного/динамічного аналізу вихідного коду. Процес сканування безпеки складається з чотирьох етапів: ідентифікація вразливостей (тестування), аналіз загроз, оцінка, санація.

Мета *ідентифікації вразливостей (тестування)* – скласти вичерпний список вразливостей програми. Аналітики безпеки перевіряють працездатність додатків, серверів або інших систем, скануючи їх за допомогою автоматизованих засобів або тестуючи їх і оцінюючи вручну.

Аналіз загроз – це практика збору, систематизації та практичного використання інформації про кіберзагрози, зазвичай організована у вигляді каналів. Аналіз загроз складається з корельованих точок даних про загрози, з якими може зіткнутися організація і які можуть варіюватися від технічних індикаторів компрометації (IoC) до докладних профілів суб’єктів кіберзагроз. Рішення про аналіз загроз складається з декількох рівнів, кожен з яких наближає дані на один крок до практичного використання:

Рівень 1. Збір даних із відкритих джерел, таких як глобальні бази даних, закриті джерела (комерційні канали досліджень кібербезпеки), а також інші ресурси в «Даркнет» (dark web).

Рівень 2. Обробка і поповнення даних для класифікації загроз, ідентифікації botnets та інших макроструктур, побудови профілів суб'єктів і груп загроз, а також виявлення загроз із конкретними шкідливими програмами.

Рівень 3. Пакування даних загроз для споживачів інформаційного потоку у вигляді каналів, що надають актуальну інформацію про нові та існуючі загрози.

Рівень 4. Використання цих даних автоматично шляхом інтеграції їх з інструментами безпеки або вручну шляхом надання співробітникам служби безпеки контекстної інформації про загрози під час аналізу або підготовки до інцидентів безпеки.

Ландшафт кібербезпеки стає все більш складним. Існують тисячі методів атаки, мільйони варіантів шкідливих програм і незліченні суб'єкти загроз та хакерські групи, які потенційно можуть загрожувати вашій організації. Аналіз загроз може допомогти:

1) бути в курсі подій – слід дізнаватися про нові загрози, що виникають, включаючи методи та інструменти;

2) ідентифікувати свого ворога – якщо ви можете пов'язати певну атаку або шкідливе програмне забезпечення з конкретною особою та зрозуміти її/його контекст та мотивацію;

3) обмінюватися інформацією – аналітика загроз надає зручно упаковану інформацію про загрози, якою ви можете поділитися з командою безпеки, а також із керівництвом та стейкхолдерами.

Розділ 2. Індикатори компрометації

Індикатори компрометації (IoCs) надають докази того, що атака мала місце, і можуть допомогти вам зрозуміти тип атаки та її джерело. Рішення для аналізу загроз використовують IoCs для швидкого підключення інцидентів кібербезпеки до відомих профілів загроз. Наприклад, якщо компанія має вихідний трафік на IP-адресу, який, як відомо, використовується для шкідливої діяльності, розвідка кіберзагроз може підключити цю IP-адресу до суб'єкта загрози і надати інформацію про шкідливі програми, що розповсюджуються цим зловмисником. Розглянемо декілька поширених прикладів індикаторів компрометації. Основним є незвичайний вихідний мережевий трафік:

1) вебтрафік, що демонструє ботоподібну поведінку;

2) незвичайні розміри HTML-відповідей;

3) велика кількість запитів на один і той самий ресурс;

4) аномальна поведінка або активність входу в систему з привілейованими обліковими записами;

5) трафік із незвичайних географічних регіонів;

6) незвична частота або обсяг даних зчитування бази даних;

7) зміни в реєстрі або системних файлах;

8) незвичайні DNS-запити або запити з незвичайного номера порту;

9) великі обсяги трафіку, що вказують на DDoS-атаку.

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це зловмисна спроба зробити онлайн-сервіс недоступним для користувачів зазвичай шляхом тимчасового переривання або припинення роботи його хост-серверу. DDoS-атака запускається з численних скомпрометованих пристроїв, часто розподілених по всьому світу в так званому bot.net. Він відрізняється від інших атак типу «відмова в обслуговуванні» (DoS) тим, що використовує один підключений до Інтернету пристрій (одне мережеве з'єднання) зі шкідливим трафіком. У цьому полягає відмінність.

DOS- і DDoS-атаки можна розділити на три типи [6]:

– *об'ємні атаки* включають UDP-floods, ICMP- flood та інші підроблені пакетні. Метою атаки є насичення трафіку атакованого сайту: зростання в бітах у секунду (біт/с);

– *протокольні атаки* включають у себе SYN floods, фрагментовані пакетні атаки, Ping of Death, Smurf DDoS та ін. Цей тип атаки «споживає» фактичні ресурси сервера або проміжного комунікаційного обладнання, такого як брандмауери і балансувальники навантаження, і вимірюється в пакетах у секунду (Pps);

– *атаки прикладного рівня* включають у себе низько- і повільні floods, GET/POST, атаки, націлені на вразливості Apache, Windows або OpenBSD, тощо.

Найбільш поширеними типами DDoS-атак є:

1. *UDP- floods* – це будь-яка DDoS-атака, яка наповнює ціль пакетами протоколу користувача Datagram Protocol (UDP) пакетами. Мета атаки – дестабілізувати випадкові порти на віддаленому хості. Це змушує хост повторно перевіряти наявність програми, що прослуховує цей порт, і (коли запит не відповідає) відповідати пакетом ICMP «Пункт призначення недосяжний». Цей процес виснажує ресурси хосту, що в кінцевому підсумку може призвести до недоступності.

2. I*CMP (Ping)* Flood схожа на атаку UDP flood, ICMP flood перевантажує цільовий ресурс пакетами ICMP Echo Request (ping), зазвичай відправляючи пакети якомога швидше, не чекаючи відповідей. Цей тип атаки може споживати як вхідний, так і вихідний трафік, оскільки сервери «жертви» часто намагаються відповісти пакетами ICMP Echo Reply, що призводить до значного загального уповільнення роботи системи.

3. DDoS-атака *SYN flood* використовує відому слабкість у послідовності TCP-з'єднань («Тристороннє рукостискання»), за яких на запит SYN для ініціювання TCP-з'єднання з хостом повинна бути отримана відповідь SYN-ACK від цього хосту, а потім підтверджена відповідь ACK. У сценарії SYN flood відправляється кілька SYN-запитів. Відповідь не находить на відповідь SYN-ACK хосту або відправляє SYN-запити з

підробленої IP-адреси. У будь-якому разі хост-система продовжує чекати підтвердження кожного із запитів, поки не вдається встановити нові з'єднання, що в кінцевому підсумку призведе до відмови в обслуговуванні.

4. Атака *Ping of death (POD)* включає у себе відправку зловмисником декількох спотворених або шкідливих pings на комп'ютер. Максимальна довжина IP-пакета (включаючи заголовок) становить 65 535 байт. Однак рівень каналу передачі даних зазвичай обмежує максимальний розмір, наприклад 1 500 байт по мережі Ethernet. У цьому разі великий IP-пакет розбивається на кілька IP-пакетів (відомих як фрагменти), і хост-одержувач повторно збирає IP-фрагменти в повний пакет. У сценарії Ping of Death після зловмисної маніпуляції вмістом фрагменту одержувач отримує IP-пакет, розмір якого за повторної збірки перевищує 65 535 байт. Це може призвести до переповнення буферів пам'яті, виділених для пакета, що призведе до відмови в обслуговуванні певних пакетів.

5. *Slowloris* – це високоцільова атака, що дає змогу одному вебсерверу знищити інший сервер, не зачіпаючи інші служби або порти у цільовій мережі. Slowloris утримує якомога більше з'єднань із цільовим вебсервером, відкритим якомога довше. Він виконує це, створюючи з'єднання із цільовим сервером, але відправляючи тільки частковий запит. Slowloris постійно надсилає більше заголовків HTTP, але ніколи не завершує запит. Цільовий сервер зберігає кожне із цих помилкових підключень відкритим. Це в підсумку переповнює максимальний паралельний пул з'єднань і призводить до відмови в додаткових з'єднаннях від законних клієнтів.

6. В атаках *посилення NTP* зловмисник використовує загальнодоступні сервери протоколу мережевого часу (NTP), щоб перевантажити цільовий сервер UDP-трафіком. Атака визначається як напад із посиленням, оскільки відношення запиту до відповіді в таких сценаріях знаходиться в проміжку між 1: 20 та 1: 200 або більше. Це означає, що будь-який зловмисник, який отримав список відкритих NTP-серверів (наприклад, за допомогою такого інструменту, як Metasploit або дані з проєкту Open NTP), може легко створити руйнівну широкосмугову, великомасштабну DDoS-атаку.

7. Під час DDoS-атаки *HTTP flood* зловмисник використовує законні HTTP GET або POST-запити для атаки на вебсервер. Http-floods не використовують спотворені пакети, методи підміни або відображення і вимагають меншої пропускної здатності, ніж інші атаки, щоб вивести з ладу цільовий сайт або сервер. Атака найбільш ефективна, коли вона змушує сервер або додаток виділяти максимально можливі ресурси у відповідь на кожний окремий запит.

8. *DDoS-атаки з нульовим днем*. Визначення «нульовий день» охоплює всі невідомі або нові атаки, які використовують вразливі місця, для яких ще не випущено жодне виправлення.

DDoS-атаки швидко стають найбільш поширеним видом кіберзагрози, за останні півтори роки швидко зростають як за кількістю, так і за обсягом [7–9]. Тенденція спрямована на зменшення тривалості атаки, але більший обсяг атак на секунду. Отже, перед відповідними фахівцями постає необхідність систематичного аналізу можливих загроз.

Розділ 3. Алгоритм виявлення загроз

Виявлення загроз зумовлює необхідність підключати аналітиків до виявлення мотивів кібератак. Основні мотиви можна представити як ідеологію, бізнес-суперечки, нудьгу, вимагання та кібервійну. Так, «хактивісти» використовують DDoS-атаки як засіб націлювання на вебсайти, з якими вони ідеологічно не згодні; «скрипт-дітки», яким нудно, використовують заздалегідь написані сценарії для запуску DDoS-атак; зловмисники використовують DDoS-атаки або загрозу DDoS-атак як засіб вимагання грошей у своїх цілей; підприємства, які використовують DDoS-атаки для стратегічного знищення вебсайтів конкурентів; уряд, якій санкціонує DDoS-атаки з метою виведення з ладу опозиційних вебсайтів та інфраструктури ворожої країни, тощо.

Одним із рішень протидії кіберзагрозам є використання Imperva, яка пом’якшує пошкодження DDoS. Imperva захищає вебсайти від DDoS-атак, вирішуючи кожен із них унікальним набором інструментів та стратегією захисту:

– *атаки на основі обсягу*. Imperva протидіє цим атакам, поглинаючи їх глобальною мережею центрів очищення, які масштабуються, на вимогу, для протидії багатогігабайтним DDoS-атакам;

– *протокольні атаки*. Imperva пом’якшує цей тип атаки, блокуючи «поганий» трафік ще до того, як він потрапляє на сайт, використовуючи технологію ідентифікації відвідувачів, яка розрізняє законних відвідувачів вебсайту (людей, пошукові системи тощо) та автоматизованих або зловмисних клієнтів;

– *атаки рівня застосунків*. Imperva пом’якшує атаки на рівні застосунків, відстежуючи поведінку відвідувачів, блокуючи відомих «поганих» ботів та кидаючи виклик підозрілим або невизнаним особам за допомогою JS-тесту, виклику cookie та навіть CAPTCHA.

У всіх цих сценаріях Imperva застосовує свої рішення захисту DDoS за межами мережі компанії, а до хостів надходить лише відфільтрований трафік. Більше того, Imperva підтримує велику базу даних про загрози DDoS, додаючі нові методи атак. Ця постійно обновлювана інформація збирається по всій мережі, виявляючи нові загрози, відомих шкідливих користувачів та застосовуючи засоби захисту в режимі реального часу на всіх захищених Imperva вебсайтах.

Imperva є одним з інструментів запобігання атакам. Однак аналітикам компанії слід періодично здійснювати моніторинг кількості атак, їх видів

та того, які нові види атак та загроз виникають. Зазвичай алгоритм виявлення загроз складається із шести етапів:

1. Направлення. На етапі направлення threat intelligence аналітик/ представник аналітичного центру розуміє, які інформаційні активи та типи інформації необхідно захистити. Представники антикризової команди разом із CEO повинні визначити, які категорії загроз можуть завдати найбільшої шкоди й які типи інформації слід захищати.

2. Збір. Фахівець компанії, якому делеговані повноваження, може збирати інформацію на вимогу компанії до аналізу загроз, включаючи: журнал даних із захищених IT-систем; існуючі канали даних загроз; бази даних та набори даних, які відомі як уразливі, або підписи шкідливого програмного забезпечення; інтерв'ю з людьми, які знають про напади або зловмисників; відкриті новини та дослідження в галузі безпеки; хакерські сайти і закриті форуми в dark web тощо.

3. Обробка. Перетворення зібраної інформації на формат даних, який може бути використаний на постійній основі для забезпечення кібер-безпеки. Якісна інформація повинна бути проаналізована, ранжована та класифікована. Кількісна інформація повинна бути переформатована в узгоджені формати. Наприклад, аналітик/аналітики кіберзагроз може збирати погані IP-адреси з журналів безпеки й упаковувати їх у CSV-файл, який можна імпортувати в інструменти безпеки з подальшою можливістю блокувати ці IP-адреси.

4. Аналіз. Після обробки інформації щодо можливих загроз вона повинна бути представлена та упакована так, щоб вона була дієвою і корисною для кінцевого користувача. Якщо одержувачі даних є професіоналами у сфері безпеки, служба аналізу загроз повинна надавати дієві точки даних, які можна використовувати в режимі реального часу для аналізу або захисту від атаки. Якщо одержувачі не є фахівцями, то інформація про загрози повинна надаватися у вигляді звітів, презентацій або відеофільмів, які пояснюють загрозу на більш доступному рівні.

5. Поширення. На етапі поширення інформація про загрози передається кінцевому користувачеві, який зможе її використати для автоматичного виявлення загроз. Інформація про загрози надається фахівцям у вигляді письмових звітів або попереджень та завантажується у систему у вигляді файлів даних у певних форматах, які підтримуються засобами безпеки.

6. Зворотний зв'язок. Важливим етапом аналізу загроз є отримання зворотного зв'язку про вплив і корисність даних. Зазвичай у компаніях робиться опитування. Питання, які виносяться до анкети, можуть бути такими: чи допомогла надана інформація зрозуміти суть проблеми; чи дасть змогу надана інформація своєчасно відреагувати та захиститися від нападу; з якими інструментами, що запропоновані в аналізі, більш ефективно працювати тощо. Отримання цього зворотного зв'язку на постійній основі може допомогти аналітикам спростити форму подачі чи зміст інформації про загрози.

Розділ 4. Інтегровані рішення для аналізу загроз

Інтегровані рішення для аналізу загроз мають чотири складники: пропозиції, аналіз уразливості, оцінку ризику та відновлення.

Будь-який аналіз має містити пропозиції щодо їх нівелювання. *Пропозиції* повинні бути інтегровані з іншими елементами, перш за все кібербезпеки. До них можна віднести:

1. Захист від DDoS-атак – необхідно підтримувати час безвідмовної роботи в усіх ситуаціях. Попередити будь-який тип атаки DDoS будь-якого розміру, щоб попередити доступ до вашого вебсайту та мережевої інфраструктури.
2. CDN (Content delivery network) – необхідно підвищити продуктивність вебсайту і скоротити витрати на пропускну здатність за допомогою CDN, призначеного для розробників. Кешування статичних ресурсів на кордоні з одночасним прискоренням роботи API і динамічних вебсайтів.
3. WAF-рішення дозволяє законний трафік і запобігає поганому трафіку, захищаючи додатки на кордоні. Gateway WAF забезпечує безпеку додатків та API всередині вашої мережі.
4. Бот-аналіз захищає ваш трафік бота з метою точного визначення аномалії, ідентифікує погану поведінку бота і перевіряє його за допомогою механізмів виклику, які не впливають на трафік користувача.
5. Безпека-захист по API. Обмеження доступу до API-інтерфейсів (відкриття API для кінцевої точки може забезпечити тільки потрібний трафік), а також виявлення і блокування спроб використання вразливостей програм.
6. Захист від захоплення облікових записів – використовує процес виявлення на основі намірів для ідентифікації та захисту від спроб захоплення облікових записів користувачів у зловмисних цілях.
7. RASP – тримайте ваші програми в безпеці зсередини від відомих атак та атак нульового дня (швидкий і точний захист без підпису або режиму навчання).
8. Аналітика атак – пом’якшення та реагування на реальні загрози кібербезпеки ефективно і точно за допомогою дієвої розвідки на всіх рівнях вашого захисту.

Наступним кроком є *аналіз уразливостей*. Мета цього кроку – визначити джерело і першопричину вразливостей, виявлених на першому етапі. Аналіз включає у себе ідентифікацію компонентів системи, відповідальних за кожну вразливість, і першопричину цієї уразливості. Наприклад, основною причиною вразливості може бути стара версія бібліотеки з відкритим вихідним кодом. Це забезпечує ясний шлях для виправлення – оновлення бібліотеки.

Оцінка ризику визначає пріоритети вразливостей. Аналітики з безпеки присвоюють ранг або оцінку важливості кожній вразливості, ґрунтуючись на відповідях на таких фактах: які системи порушені; які

дані знаходяться в зоні ризику; які бізнес-функції піддаються ризику; атаки або компроміс; тяжкість нападу; потенційний збиток у результаті уразливості.

Відновлення. Метою цього кроку є усунення прогалин у сфері безпеки. Як правило, це спільні зусилля співробітників служби безпеки, розробників та оперативних груп, які визначають найбільш ефективний шлях усунення або пом'якшення кожної уразливості. Конкретні кроки по відновленню можуть включати в себе:

1) упровадження нових процедур, заходів або інструментів забезпечення безпеки;
2) оновлення операційних або конфігураційних змін;
3) розроблення та впровадження патча вразливості;
4) оцінка вразливості не може бути одноразовим заходом.

Щоб бути ефективними, компанії повинні ввести цей процес у дію і регулярно повторювати його. Окрім того, вкрай важливо розвивати співпрацю між групами з питань безпеки, експлуатації та розроблення – процес, відомий як DevSecOps.

DevSecOps – це культурний зсув в індустрії програмного забезпечення, спрямований на те, щоб перетворити безпеку на цикли швидкого випуску, типові для сучасного розроблення і розгортання додатків, також відомі як рух DevOps [10]. Прийняття цього менталітету зсуву вліво вимагає від компаній подолання розриву, який зазвичай існує між командами розроблення і безпеки, до такого ступеню, що багато процесів безпеки автоматизуються й обробляються самою командою розроблення.

Традиційно великі розробники програмного забезпечення випускали нові версії своїх додатків кожні кілька місяців або навіть років. Це дало достатньо часу для того, щоб код пройшов перевірку якості та безпеки, процесів, які виконувалися окремими спеціалізованими групами, як внутрішніми, так і зовнішніми підрядниками. Проте в останні десять років спостерігається зростання публічних хмар, контейнерів і мікросервісної моделі, де монолітні додатки розбиваються на більш дрібні частини, які працюють незалежно. Ця розбивка також мала безпосередній вплив на те, як розробляється програмне забезпечення, що призвело до перехідних випусків і гнучкої практики розроблення, де нові функції і код постійно впроваджуються у виробництво швидкими темпами. Багато із цих процесів було автоматизовано з використанням нових технологій та інструментів, що дало змогу компаніям швидше впроваджувати інновації та залишатися попереду конкурентів.

Розвиток хмарних технологій, контейнерів і мікросервісів також призвів до появи культури DevOps, завдяки якій розробники можуть надавати і масштабувати необхідну їм інфраструктуру, не чекаючи, поки за них це зробить окрема команда розробників інфраструктури. Усі основні хмарні провайдери тепер пропонують API та інструменти

налаштування, які дають змогу розглядати конфігурацію інфраструктури як код із використанням шаблонів розгортання.

Тоді як культура DevOps принесла багато інновацій у розроблення програмного забезпечення, безпека часто не могла йти в ногу з новою швидкістю, з якою створювався і випускався код. DevSecOps – це спроба виправити це і повністю інтегрувати тестування безпеки в конвеєри безперервної інтеграції (CI) і безперервної доставки (CD), а також накопичити знання і навички, необхідні в команді розробників, щоб результати тестування і виправлення також могли бути зроблені всередині компанії.

Усе більше компаній інтегрують автоматизовані перевірки безпеки як частину конвеєрів CI/CD, але результати можуть бути не відразу очевидні через те, що він називається «обов'язком безпеки», тобто кількістю вразливостей, які потрапляють у виробництво, тому що розробники вирішили не виправляти їх. Це може статися із цілої низки причин, включаючи неможливість виправити їх негайно, не плануючи коли-небудь їх виправляти, тому що є інші пом'якшувальні заходи або тому що вони мають меншу ступінь загрози.

У своєму звіті про стан безпеки програмного забезпечення за 2020 р., що побудований на даних, зібраних у ході сканування 85 тис додатків протягом року, Veracode показує, що середній час виправлення вразливостей, виявлених у додатках, становить 171 день порівняно із середнім часом 59 днів десять років тому, коли вийшов перший звіт. Під час кореляції результатів сканування з частотою сканування для певної програми (збільшення частоти передбачає інтеграцію автоматизованого сканування в робочі процеси CI/CD) дані показують, що додатки, скановані щодня, мають середній час фіксації 19 днів порівняно із 68 днями для додатків, які скануються щомісяця [11]. Це говорить про те, що часте сканування підвищує ймовірність швидкого виправлення вразливостей.

Ще однією перевагою справжньої зміни культури до DevSecOps має бути те, що кількість серйозних уразливостей, що існують у коді, також повинно зменшитися. Дані Veracode показують, що відсоток додатків без уразливостей фактично знизився, припускаючи, що ситуація погіршилася, але відсоток додатків без дефектів високого ступеня серйозності фактично збільшився із 66% до 80% [11].

Додатково можна використати інструменти оцінки вразливостей, які призначені для автоматичного пошуку нових та існуючих загроз і можуть бути націлені на ваш додаток. Типи інструментів включають у себе:

1) сканери вебдодатків, які перевіряють та імітують відомі шаблони атак;
2) сканери протоколів, які шукають уразливі протоколи, порти та мережеві служби;

3) мережеві сканери, які допомагають візуалізувати мережі та виявляти попереджувальні сигнали, такі як випадкові IP-адреси, підроблені пакети та підозріла генерація пакетів з однієї IP-адреси.

Результати цих перевірок повинні бути включені в поточний процес оцінки вразливості організації. Брандмауер вебдодатків допомагає захистити від уразливостей додатків кількома способами:

1. Будучи шлюзом для всього вхідного трафіку, він може активно відфільтрувати шкідливих відвідувачів і запити, такі як SQL-ін'єкції і XSS-атаки. Це виключає ризик передачі даних зловмисникам.

2. Він може виконувати віртуальне виправлення – автоматичне застосування виправлення для знову виявленої вразливості на кордоні мережі, що дає розробникам і IT-командам можливість безпечно розгорнути новий патч у додатку без будь-яких проблем.

3. WAF надає уявлення про події безпеки. Аналітика атак допомагає контекстуалізувати атаки та виявляти загальні загрози (наприклад, показуючи тисячі, здавалося б, незв'язаних атак як частину однієї великої кампанії атак).

4. WAF інтегрується з усіма провідними Siem-платформами, щоб надати компанії чітке уявлення про загрози, з якими вони стикаються, і допомогти підготуватися до нових атак.

Розділ 5. Керівництво з оцінки вразливостей

Проведений аналіз дасть змогу використати метод запуску ефективного процесу оцінки вразливості з використанням будь-якого автоматизованого або ручного інструменту. Першочерговим завданням є визначення ризиків, а також їх критичне значення.

Наступним кроком є визначення базової лінії системи: збір інформації про системи до проведення оцінки вразливостей. На цьому етапі зазвичай відбувається перевірка на пристроях відкритих портів та процесів, які не повинні бути відкриті, вивчення затверджених драйверів та програмного забезпечення, вивчення базової конфігурації кожного пристрою, виконання захоплення банеру або визначення, яка «загальнодоступна» інформація повинна бути доступна на основі базової конфігурації, тощо.

Третій крок – сканування вразливостей. На цьому етапі використовують правильну політику сканера для досягнення бажаних результатів. Перш ніж розпочати перевірку вразливості, здійснюється співставлення критеріїв оцінки до рівня відповідності вимогам компанії. Важливо розпізнати контекст галузі функціонування компанії та визначити можливість одночасного виконання сканування без застосування сегментації.

Прикладами найкращих результатів використання відповідних інструментів та плагінів на платформі оцінки вразливості можуть бути:

1. Використання популярних портів.

2. Вебсканування CMS (Joomla, WordPress, Drupal, загальна CMS тощо).

3. Швидке сканування.
4. Сканування брандмауера.
5. Стелс-сканування.
6. Агресивне сканування.
7. Повне сканування, використання та розподілені атаки відмови в обслуговуванні (DDoS).
8. Відкриття проєкту безпеки вебдодатків (OWASP).
9. Підготовка вебдодатків до стандарту безпеки даних платіжних карток (PCI DSS).
10. Перевірка політики безпеки на дотримання/виконання закону про переносимість та підзвітність медичного страхування (HIPAA) на предмет відповідності вимогам.

Використання ручного сканування критичних ресурсів із метою забезпечення найкращих результатів слід здійснювати після налаштування облікових даних у конфігурації сканера.

Четвертий крок – створення звіту про оцінку вразливості. Під час підготовки звіту необхідно:

– надати рекомендації з метою отримання реальної цінності у підсумковому звіті;

– надати рекомендації на основі початкових цілей оцінки;

– запропонувати методи зменшення ризику на основі критичності активів та результатів;

– надати висновки, пов’язані з будь-яким можливим розривом між результатами та визначенням базової лінії системи (відхилення в будь-якій неправильній конфігурації та зроблені відкриття), та рекомендації щодо виправлення відхилень і пом’якшення можливих уразливостей.

Однак важливо мати на увазі такі деталі та усвідомлювати, що високі та середні вразливості повинні мати детальний звіт, який може містити: назву вразливості, дату відкриття, оцінку на основі баз даних загальних уразливостей та ризиків (CVE), детальний опис уразливості, деталі щодо уражених систем, детальну інформацію про процес усунення вразливості, доказ концепції (PoC) вразливості для системи (якщо це можливо), порожнє поле для власника вразливості, час, необхідний для її виправлення, наступну ревізію і контрзаходи між рішеннями.

Озброївшись цим базовим переліком під час проведення оцінки вразливості, етап рекомендацій відображатиме повне розуміння положення щодо безпеки в усіх аспектах процесу.

Для візуалізації описаного процесу використаємо платформу Smartsheet [12]. Платформою можуть користуватися зареєстровані користувачі. Для початківців на головній сторінці розміщено мануал та покрокові відеоінструкції. Сервіс зручний у використанні. Окрім того, формуються зручні читабельні звіти, існує можливість додавати файли, які не слід пересилати поштою кінцевому адресату, та кольорові заливки,

які визначають ступінь загрози. Скористаємося шаблонами платформи і почнемо будувати план усунення виявлених уразливостей (рис. 1).

PROTECTED ASSET	RISK	POSSIBLE THREATS	COMPROMISING AREAS OF	CONSEQUENCE OF BREACH	RISK SEVERITY	RISK LIKELIHO	RISK LEVEL
					ACCEPTABLE	IMPROBABLE	LOW
					TOLERABLE	POSSIBLE	MEDIUM
					UNDESIRABLE	PROBABLE	HIGH
					INTOLERABLE	PROBABLE	EXTREME

Рис. 1. План усунення виявлених уразливостей

Джерело: [12]

Усі визначені першочергові загрози (активи, які слід захищати) або потенційні загрози (наприклад, хакери, колишні співробітники або інші неавторизовані користувачі) й уразливості (наприклад, недостатні паролі, програмні помилки та доступ співробітників до конфіденційних даних) вносяться в перший стовпчик, у другому стовпчику відображається ризик відповідно до визначеної в компанії шкали. На платформі наведено параметри визначення певних «показників» (рис. 2).

Першими, хто запропонував використовувати кольорове фарбування ячейок у талицях, були аналітики Фонду нової економіки, які в 2006 р. розробили за пропонували The Happy Planet Index (HPI) [13]. Ця технологія суттєво спросила сприйняття великих таблиць із даними. Такі визуалізовані звіти допомогають сприймати ступінь ризику та загроз і швидкість реакції на них.

Після оцінки рівнів ризику та впливу необхідно визначити пріоритет кожного запису та створити плани вирішення проблем (рис. 3).

Як ми бачимо з рисунку 3, мінімальному рівню чи то загроз, чи то пріоритетів відповідає зелений колір, максимальному – червоний. Цей шаблон призначений для того, щоб допомогти визначити та вирішити проблеми безпеки, пов’язані з інформаційними технологіями. Платформа дає змогу оцінювати елементи одного IT-ресурсу, наприклад вебсайту, або виконувати оцінку вразливості для всієї організації, розглядаючи ризики для мережі, сервера, брандмауера або конкретних наборів даних.

Після введення основних ризиків, визначення пріоритетів та їх рівнів відбувається генерація шаблону (рис. 4).

RISK RATING KEY	LOW	MEDIUM	HIGH	EXTREME
	0 – ACCEPTABLE OK TO PROCEED	1 – ALARP (as low as reasonably practicable) TAKE MITIGATION EFFORTS	2 – GENERALLY UNACCEPTABLE SEEK SUPPORT	3 – INTOLERABLE PLACE EVENT ON HOLD

	SEVERITY			
	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW – 1 –	MEDIUM – 4 –	MEDIUM – 6 –	HIGH – 10 –
POSSIBLE RISK WILL LIKELY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 11 –
PROBABLE RISK WILL OCCUR	MEDIUM – 3 –	HIGH – 7 –	HIGH – 9 –	EXTREME – 12 –

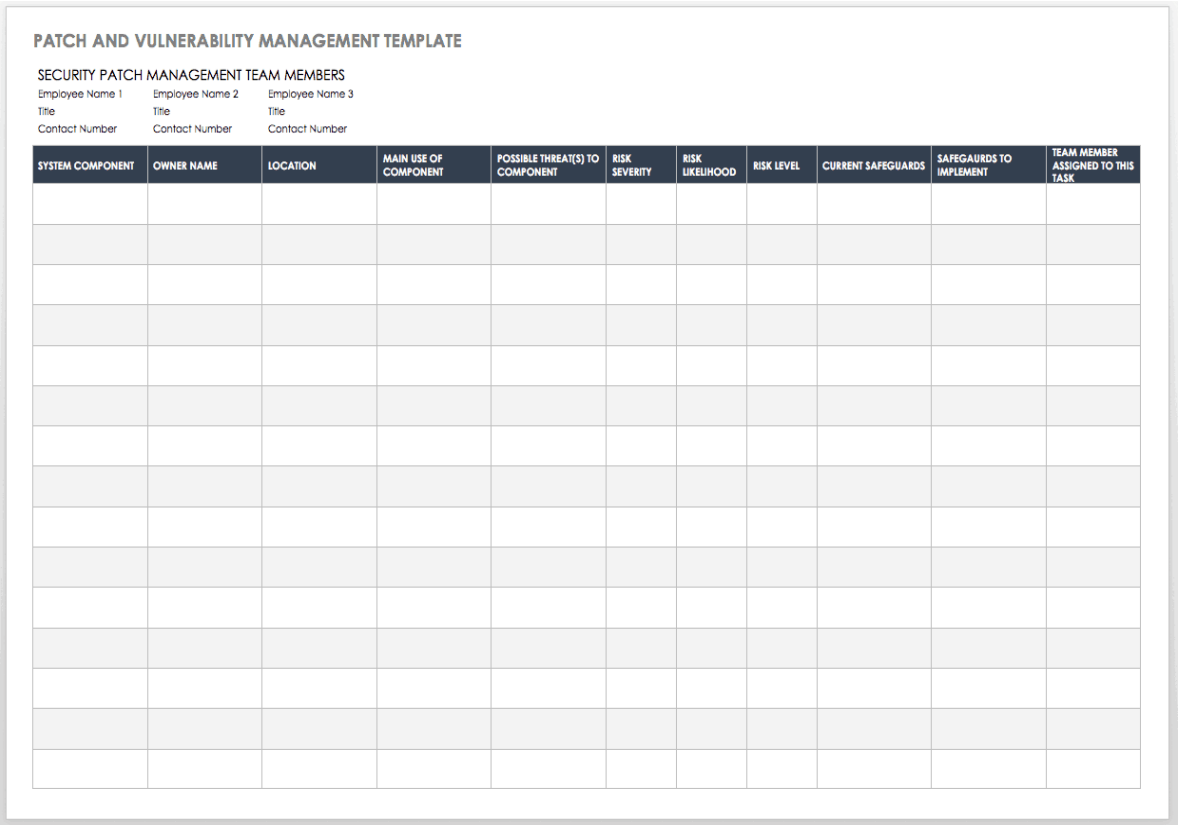
Рис. 2. Параметри визначення певних «показників»

Джерло: [12]

CURRENT SAFEGUARDS	PROPOSED SAFEGAURDS	PRIORITY	TEAM MEMBER	DUE DATE	RISK SEVERITY	RISK LIKELIHOO	RISK LEVEL KEY
		LOW			ACCEPTABLE	IMPROBABLE	LOW
		LOW			TOLERABLE	POSSIBLE	MEDIUM
		MEDIUM			UNDESIRABLE	PROBABLE	HIGH
		HIGH			INTOLERABLE		EXTREME

Рис. 3. Визначення рівнів пріоритетів загроз [12]

Джерло: [12]



PATCH AND VULNERABILITY MANAGEMENT TEMPLATE

SECURITY PATCH MANAGEMENT TEAM MEMBERS

Employee Name 1	Employee Name 2	Employee Name 3
Title	Title	Title
Contact Number	Contact Number	Contact Number

SYSTEM COMPONENT	OWNER NAME	LOCATION	MAIN USE OF COMPONENT	POSSIBLE THREAT(S) TO COMPONENT	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	CURRENT SAFEGUARDS	SAFEGAURDS TO IMPLEMENT	TEAM MEMBER ASSIGNED TO THIS TASK

Рис. 4. Шаблон плану управління виправленнями та вразливостями

Джерло: [12]

Цей шаблон процесу управління вразливостями надає базову схему для створення власного комплексного плану. Документування процедур управління виправленнями є життєво важливою частиною забезпечення кібербезпеки: створюючи план управління виправленнями та вразливостями, компанії можуть допомогти гарантувати, що IT-системи не будуть скомпрометовані. Шаблон включає розділи, що описують обсяг плану управління, відповідні ролі та обов'язки, політику, якій необхідно слідувати, методи ранжирування ризиків і кроки щодо виправлення становища. Ви також можете включити інвентаризацію конкретних компонентів системи або іншу інформацію, засновану на ваших бізнес-потребах.

Другий згенерований шаблон – шаблон плану усунення вразливостей (рис. 5).

Шаблон плану дій з оцінки вразливості фокусується на усуненні вразливостей. Перерахуйте слабкі місця, які необхідно усунути, а також плани щодо усунення вразливостей, терміни та основні етапи, рівні ризику та оновлення статусу. Далі відбувається аналіз вразливості компанії і генерується відповідний шаблон (рис. 6).

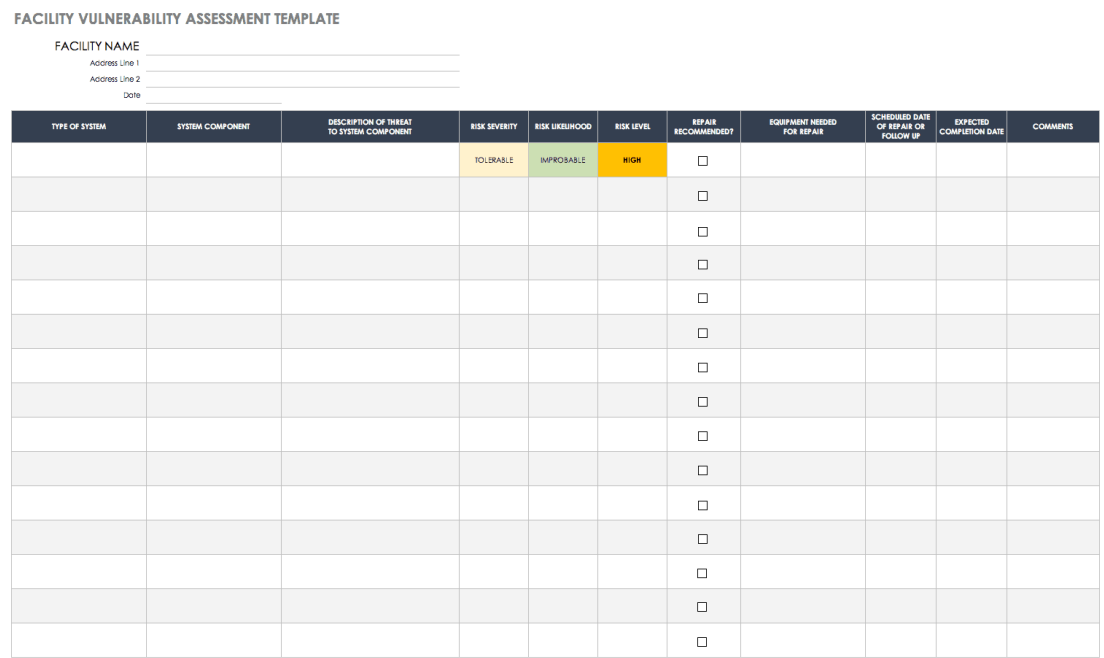
VULNERABILITY REMEDIATION PLAN TEMPLATE

CLIENT NAME
Address Line 1
Address Line 2
Date

SYSTEM COMPONENT	TEAM MEMBER ASSIGNED TO THIS TASK	MAIN USE OF COMPONENT	COMPONENT WEAKNESS DESCRIPTION	HARDWARE NEEDED FOR PATCH/REPAIR	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	MILESTONE 1	MILESTONE 2	MILESTONE 3	EXPECTED COMPLETION DATE	COMMENTS
					TOLERABLE	IMPROBABLE	HIGH					

Рис. 5. Шаблон плану усунення вразливостей

Джерло: [12]



FACILITY VULNERABILITY ASSESSMENT TEMPLATE

FACILITY NAME
Address Line 1
Address Line 2
Date

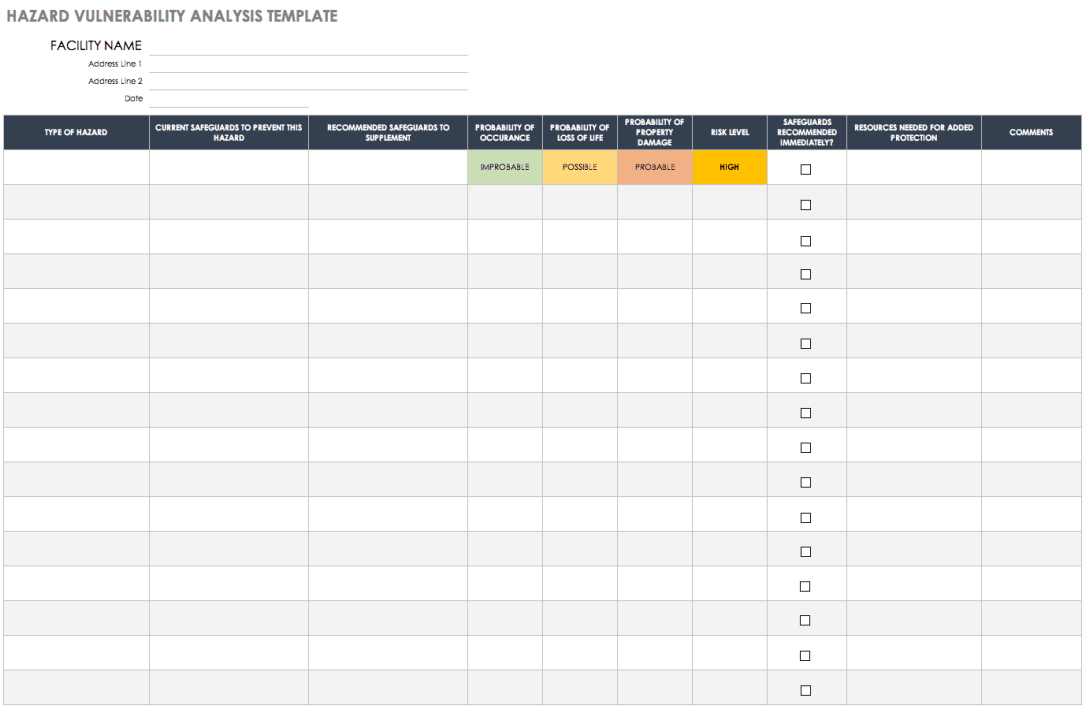
TYPE OF SYSTEM	SYSTEM COMPONENT	DESCRIPTION OF THREAT TO SYSTEM COMPONENT	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	REPAIR RECOMMENDED?	EQUIPMENT NEEDED FOR REPAIR	SCHEDULED DATE OF REPAIR OR FOLLOW UP	EXPECTED COMPLETION DATE	COMMENTS
			TOLERABLE	IMPROBABLE	HIGH	☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				
						☐				

Рис. 6. Шаблон оцінки вразливості компанії

Джерло: [12]

Шаблон оцінки вразливості компанії дає змогу перерахувати критичні частини з метою визначення головних пріоритетів під час оцінки вразливості. Виявлення цих важливих компонентів також може допомогти краще зрозуміти потенційні загрози. Шаблон призначений для того, щоб допомогти оцінити ризик на основі ймовірності виникнення загроз, серйозності впливу, який ці загрози можуть створити, і визначити ефективність поточних заходів безпеки компанії.

Здійснивши оцінку вразливості, слід згенерувати шаблон аналізу вразливості небезпеки (рис. 7).



HAZARD VULNERABILITY ANALYSIS TEMPLATE

FACILITY NAME
Address Line 1
Address Line 2
Date

TYPE OF HAZARD	CURRENT SAFEGUARDS TO PREVENT THIS HAZARD	RECOMMENDED SAFEGUARDS TO SUPPLEMENT	PROBABILITY OF OCCURANCE	PROBABILITY OF LOSS OF LIFE	PROBABILITY OF PROPERTY DAMAGE	RISK LEVEL	SAFEGUARDS RECOMMENDED IMMEDIATELY?	RESOURCES NEEDED FOR ADDED PROTECTION	COMMENTS
			IMPROBABLE	POSSIBLE	PROBABLE	HIGH	☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		
							☐		

Рис. 7. Шаблон аналізу вразливості небезпеки

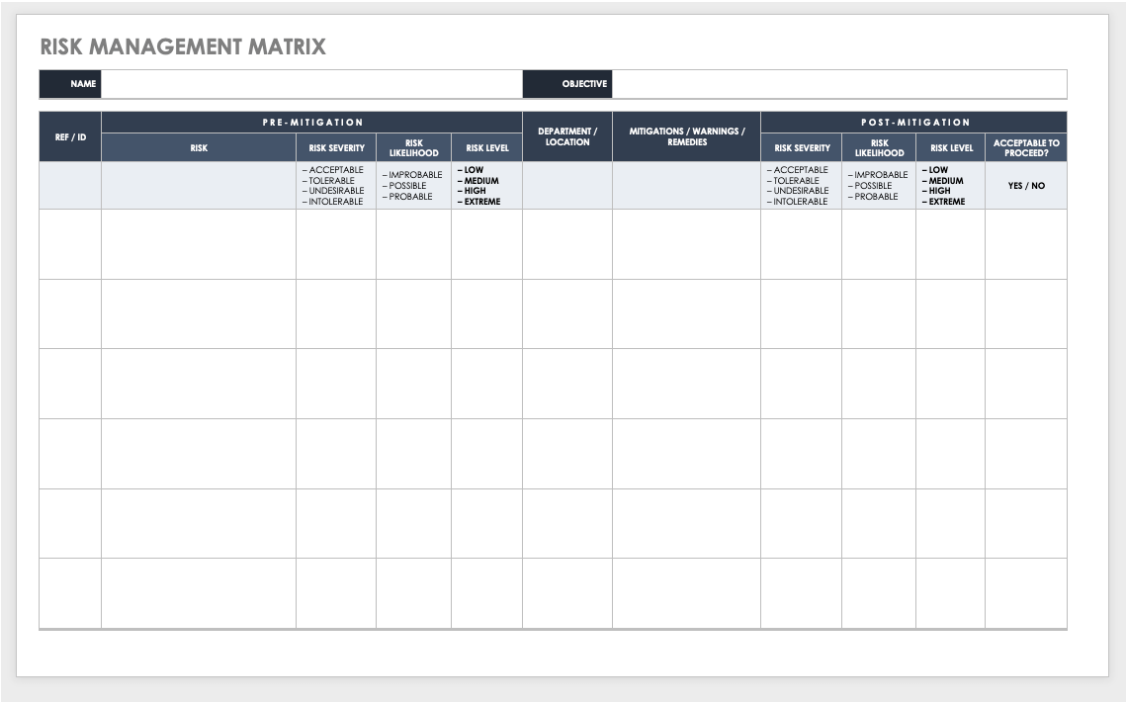
Джерело: [12]

Діапазон можливих небезпек величезний, але на діяльність більшості компаній можуть негативно вплинути такі загрози, як стихійне лихо, відключення електроенергії, пожежа або злочинна діяльність (пограбування або витік даних). Незалежно від того, які небезпеки можуть виникнути, цей шаблон може допомогти розставити пріоритети і підготуватися до них. Перш за все слід визначити ймовірність, вплив і поточний рівень готовності компанії на певні виклики. Саме цим займається антикризова команда: проводить тренінги та допомагає підготуватися до радикальних подій або «форс-мажорів», щоб звести до мінімуму негативний вплив або наслідки. Команда повинна також зробити ранжування ризиків, які відображаються в матриці (рис. 8).

Матриця ризиків – це швидкий інструмент для оцінки та ранжирування ризиків. Цей шаблон поєднує у собі матрицю з управлінського планування, що дає змогу оцінити рівень ризику до і після антикризових заходів, надати рекомендації та визначити, коли ризик буде усунений. Це простий спосіб організації та оцінки ризиків для будь-якої компанії.

Останній крок – формування звіту про оцінку вразливості. Як приклад застосовуємо шаблон (Додаток 1). Розроблений для оцінки всієї організації звіт про вразливості дає змогу структурувати інші загрози і вразливості, пов’язані з персоналом, операціями, будівлями та іншими

об’єктами, IT-безпекою та іншими факторами. Шаблон також містить місце для плану дій щодо усунення виявлених вразливостей.



RISK MANAGEMENT MATRIX

NAME		OBJECTIVE	

REF / ID	PRE-MITIGATION				DEPARTMENT / LOCATION	MITIGATIONS / WARNINGS / REMEDIES	POST-MITIGATION			
	RISK	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL			RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	ACCEPTABLE TO PROCEED?
		– ACCEPTABLE – TOLERABLE – UNDESIRABLE – INTOLERABLE	– IMPROBABLE – POSSIBLE – PROBABLE	**– LOW** **– MEDIUM** **– HIGH** **– EXTREME**			– ACCEPTABLE – TOLERABLE – UNDESIRABLE – INTOLERABLE	– IMPROBABLE – POSSIBLE – PROBABLE	**– LOW** **– MEDIUM** **– HIGH** **– EXTREME**	YES / NO

Рис. 8. Матриця ризиків

Джерело: [12]

Висновки

Отже, оцінка вразливості системи безпеки дає змогу компаніям вивчити й усунути вразливості до того, як вони стануть проблематичними. Швидка зміна технологій вимагає проведення оцінок на регулярній основі. Під час здійснення оцінки слід визначати: 1) слабкість у системі, яка може призвести до порушення безпеки або інших негативних наслідків, якщо її використовувати (навмисно, випадково або випадково, наприклад у разі стихійного лиха); 2) події або умови, які можуть завдати шкоди або іншим чином мати несприятливий вплив на актив. Загрози можуть бути навмисними діями, такими як крадіжка хакерами інформації про кредитні картки, випадкова подія або екологічна подія; способи, якими система може бути порушена загрозою, та серйозність цих наслідків; потенційна можливість знешкодити загрозу.

Оцінка вразливості зазвичай розглядає потенційні загрози, уразливості системи і вплив, щоб визначити основні слабкі місця, які необхідно усунути. Оцінка ризиків – це окремий, але взаємопов’язаний захід, який також розглядає ймовірні загрози та вплив із метою пом’якшення потенційних проблем.

Хоча існують відмінності під час оцінки вразливостей матеріальних цінностей та Інтернет-безпеки, основні кроки в оцінці вразливості та управлінні нею включають:

1) *оцінку загроз*: процес виявлення потенційних загроз і дій, які можуть мати місце. Вид загрози може варіюватися від хакерської атаки до недостатньо підготовленого співробітника, нападу терористу або стихійного лиха;

2) *оцінку вразливості:* визначення слабких місць, які є вразливими. Повільна реакція на слабкі місця підвищує ймовірність впливу на систему або актив. Уразливості будуть варіюватися залежно від типу системи та її складності: відсутність збору ідентифікаторів співробітників після звільнення, неадекватне захисне обладнання на об'єкті, проблеми з брандмауером і неадекватне навчання персоналу, активний обліковий запис у системі після звільнення людини тощо;

3) *оцінку ймовірності та впливу*: ранжування на основі комбінації ймовірності та впливу. Під час оцінки впливу враховується ступінь впливу на організацію або актив у разі виникнення вразливості. Наприклад, наслідки відключення електроенергії можуть призвести до зниження доходів, утрати даних або серйозних травм залежно від типу бізнесу і виконуваної роботи. Ймовірність та вплив можуть бути оцінені від високої до низької. Кількісну оцінку вразливостей та загроз слід додати до антикризового плану компанії;

4) *вироблення рекомендацій*: після проведення та аналізу оцінки розробляється план усунення вразливостей (упровадження більш надійних паролів або переобладнання будівлі для підвищення безпеки);

5) *переоцінку*: нові загрози і вразливості можуть виникнути в міру усунення інших. Після виконання рекомендацій важливо постійно проводити переоцінку системи, проводити тренінги та симуляції «а якби було прийнято інше рішення».

Список використаних джерел:

1. ISO/IEC 27000 Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь. ISO/IEC. 20.10.2019. URL: http://pqmonline.com/assets/files/pubs/translations/std/iso-mek27000-2016.pdf (дата звернення: 19.12.2021).
2. Understanding NIMS and ICS. URL: https://www.aspcapro.org/resource/understanding-nims-and-ics (accessed: 10.12.2021).
3. Козаченко П.П., Панаско О.М. Управління інцидентами в контексті інформаційної безпеки підприємства. *ΛΟΓΟΣ.* С. 119–120. DOI: https://doi.org/10.36074/11.12.2020.v2.33. URL: https://ojs.ukrlogos.in.ua/index.php/logos/article/view/7127 (дата звернення: 01.12.2021).
4. Ревізорова К., Гріненко Т. Оцінка критичності вразливостей в операційних системах. *Global Cyber Security Forum :* матеріали Першого міжнародного науково-практичного форуму, 14–16 листопада 2019 р. Харьків : ХНУРЕ, 2019. С. 86–87. URL: https://openarchive.nure.ua/bitstream/document/10553/1/REVIZOROVA.pdf (дата звернення: 19.11.2021).

5. GSA IT Schedule 70 : website. URL: https://www.igov.com/gsa-schedule-70.html (accessed: 10.11.2021).
6. Distributed denial of service attack (DDoS) definition : website: URL: https://www.imperva.com/learn/ddos/ddos-attacks/ (accessed: 19.11.2021).
7. Купреев О., Бадовская Е., Гутников А. DDoS-атаки в I квартале 2021 года. URL: https://securelist.ru/ddos-attacks-in-q1-2021/101390/ (дата звернення: 19.11.2021).
8. Купреев О., Бадовская Е., Гутников А. DDoS-атаки в IV квартале 2020 года. URL: https://securelist.ru/ddos-attacks-in-q4-2020/100469/ (дата звернення: 19.11.2021).
9. Купреев О., Бадовская Е., Гутников А., Шмелев Я. DDoS-атаки во II квартале 2021 года. URL: https://securelist.ru/ddos-attacks-in-q2-2021/102607/ (дата звернення: 19.11.2021).
10. DevSecOps: web site. URL: https://www.ibm.com/ru-ru/cloud/learn/devsecops (accessed: 20.12.2021).
11. Manage Your Entire Application Security Program in a Single Platform: web site. URL: https://www.veracode.com/ (accessed: 20.12.2021).
12. Smartsheet: web site. URL: https://www.smartsheet.com/marketplace/template-gallery#sort=relevancy&numberOfResults=24&f:@app_type=[Template,Template-Set]&f:@language=[English] (accessed: 20.12.2021).
13. The Happy Planet Index: web site. URL: https://web.archive.org/web/20090926174209/http://www.happyplanetindex.org/ (accessed: 20.12.2021).

References:

1. ISO/IEC 27000 Informatsionnyye tekhnologii – Metody i sredstva obespecheniya bezopasnosti – Sistemy menedzhmenta informatsionnoy bezopasnosti – Obshchiye svedeniya i slovar. ISO/IEC [ISO/IEC 27000 Information technology – Security techniques and tools – Information security management systems – General information and vocabulary. ISO/IEC]. 20.10.2019: web-site. Available at: http://pqmonline.com/assets/files/pubs/translations/std/iso-mek27000-2016.pdf.
2. Understanding NIMS and ICS. URL: web-site. Available at: https://www.aspcapro.org/resource/understanding-nims-and-ics (accessed: 10.12.2021).
3. Kozachenko P.P., Panasko O.M. Upravlinnya intsydentamy v konteksti informatsiynoyi bezpeky pidpryyemstva [Kozachenko R, Panasko O. Incident management in the context of enterprise information security]. *Zbirnyk naukovykh prats' LÓHOS* [Collection of scientific works ΛÓΓΟΣ]. Available at: https://ojs.ukrlogos.in.ua/index.php/logos/article/view/7127 DOI 10.36074/11.12.2020.v2.33 (accessed: 01.12.2021).
4. Revizorova K., Hrinenko T. Otsinka krytychnosti vrazlyvostey v operatsiynykh systemakh [Revizorova K. Grinenko T. Evaluation of criticality of vulnerabilities in operating systems]. *Global Cyber Security Forum:* materialy Pershoho mizhnarodnoho naukovo-praktychnoho forumu [materials of the First International Scientific and Practical Forum, November 14 – 16, 2019 – Kharkiv: KhNURE], 14–16 lystopada 2019 r. – Khar′kiv: KHNURE. Available at: https://openarchive.nure.ua/bitstream/document/10553/1/REVIZOROVA.pdf.
5. GSA IT Schedule 70: Web site. Available at: https://www.igov.com/gsa-schedule-70.html.
6. Distributed denial of service attack (DDoS) definition. Available at: https://www.imperva.com/learn/ddos/ddos-attacks.
7. Kupreyev O., Badovskaya Ye., Gutnikov A. DDoS-ataki v I kvartale 2021 goda [Kupreev O., Badovskaya E., Gutnikov A. DDoS attacks in Q1 2021]. Available at: https://securelist.ru/ddos-attacks-in-q1-2021/101390.

8. Kupreyev O., Badovskaya Ye., Gutnikov A. DDoS-ataki v IV kvartale 2020 goda [Kupreev O., Badovskaya E., Gutnikov A. DDoS attacks in Q4 2020]. Available at: https://securelist.ru/ddos-attacks-in-q4-2020/100469.
9. Kupreyev O., Badovskaya Ye., Gutnikov A., Shmelev YA. DDoS-ataki vo II kvartale 2021 goda [Kupreev O., Badovskaya E., Gutnikov A., Shmelev Y. DDoS attacks in Q2 2021]. Available at: https://securelist.ru/ddos-attacks-in-q2-2021/102607.
10. DevSecOps: web site. Available at: https://www.ibm.com/ru-ru/cloud/learn/devsecops.
11. Manage Your Entire Application Security Program in a Single Platform: web site. Available at: https://www.veracode.com.
12. Smartsheet: web site. URL: https://www.smartsheet.com/marketplace/template-gallery#sort=relevancy&numberOfResults=24&f:@app_type=[Template,Template-Set]&-f:@language=[English].
13. The Happy Planet Index: web-site. Available at: https://web.archive.org/web/20090926174209/http://www.happyplanetindex.org.

Додаток 1

ШАБЛОН

Звіт
про оцінку вразливостей

назва компанії

адреса

web address

VERSION 0.0.0.

00/00/00

Історія				
ВЕРСІЯ	**СХВАЛЕНО**	**ДАТА ВИПУСКУ**	**ОПИС ЗМІН**	**АВТОР**

ПІДГОТОВЛЕНО		**НАЗВА**		**ДАТА**	
СХВАЛЕНО		**НАЗВА**		**ДАТА**	

ЗМІСТ