Управління ризиками

Управління IT-безпекою визначає, хто уповноважений ухвалювати рішення щодо кіберризиків в організації. Управління IT-безпекою показує відповідальність і забезпечує нагляд, щоб гарантувати, що будь-які ризики належним чином знижуються, а стратегії безпеки узгоджуються з бізнес-цілями організації та відповідають правилам.
Управління IT-безпекою не слід плутати з управлінням інформаційною безпекою, що визначає та реалізує засоби контролю, які організація повинна мати для зменшення ризиків. Аналогічно, **управління даними**, зокрема, визначає, хто уповноважений приймати рішення щодо даних в організації.

Власник даних
: Особа, яка забезпечує дотримання політик та процедур, класифікує інформаційні активи та визначає критерії доступу до інформаційних активів.

Контролер даних
: Особа, яка визначає цілі та спосіб обробки персональних даних.

Обробник даних
: Особа або організація, яка обробляє персональні дані від імені контролера даних.

Зберігач даних
: Особа, яка контролює класифікацію та безпеку даних, відповідно до встановлених власником даних правил. Іншими словами, зберігач даних відповідає за технічний контроль даних.

Адміністратор даних
: Особа, яка гарантує, що дані підтримують бізнес-потреби організації та відповідають нормативним вимогам.

Фахівець з питань захисту даних
: Особа, яка наглядає за стратегією захисту даних в організації.

Політика кібербезпеки — це високорівневий документ, в якому викладено бачення кібербезпеки в організації, включаючи цілі, потреби, зміст та відповідальність. Зокрема, документ:

- Вказує на прихильність організації до вимог безпеки.
- Встановлює стандарти поведінки та вимоги безпеки для здійснення діяльності, процесів і операцій, а також для захисту технологій та інформаційних активів в організації.
- Забезпечує узгоджене придбання, використання та обслуговування операційних систем, програмного та апаратного забезпечення в усій організації.
- Визначає правові наслідки порушення політики.
- Надає команді безпеки необхідну підтримку від вищого керівництва.

Існують різні типи політик кібербезпеки.

Типи політик безпеки

Організація повинна встановити чіткі та детальні політики безпеки, що доведені до відома усіх співробітників. Важливо, щоб ці політики також підтримувалися вищим керівництвом.

Політика ідентифікації та аутентифікації
: Визначає того, кому може бути надано доступ до мережних ресурсів, а також вказує на існуючі процедури перевірки, які цьому сприяють.

Політика використання паролів
: Визначає мінімальні вимоги до пароля, такі як кількість і тип використовуваних символів, а також частота їх зміни.

Політика прийнятного використання
: Висвітлює сукупність правил, які визначають доступ до мережних ресурсів та їх використання. Також може визначати наслідки порушення політики.

Політика віддаленого доступу
: Вказує, як віддалено підключитися до внутрішньої мережі організації, та пояснює, яка інформація доступна віддалено.

Політика обслуговування мережі
: Описує процедури оновлення обраних організацією операційних систем та програм кінцевих користувачів.

Політика обробки інциденту
: Надає рекомендації щодо того, як повідомляти та реагувати на інциденти, пов’язані з безпекою в організації.

Політика даних
: Встановлює вимірювані правила обробки даних в організації, наприклад, вказує, де зберігати дані, як дані класифікувати (висококонфіденційні, середньоконфіденційні, низькоконфіденційні, конфіденційні, публічні чи приватні), а також, як дані обробляти та як дані видаляти.

Політика повноважень
: Забезпечує виконання правил створення облікових записів, наприклад, мінімальної та максимальної довжини пароля.

Організаційна політика
: Надає рекомендації щодо того, як потрібно виконувати роботу в організації. Приклади можуть містити політики управління змінами, контролю змін або управління активами.

Політика інформаційної безпеки (відео)
https://youtu.be/ZlKgMUOpMf8

Основні вразливості комп'ютерної безпеки
https://www.n-able.com/features/computer-security-vulnerabilities

Написання IT-політик безпеки технічною мовою за п'ять простих кроків
https://www.sans.org/reading-room/whitepapers/policyissues/technical-writing-security-policies-easy-steps-492

Десять заповідей комп'ютерної етики



Етика фахівця з кібербезпеки

Етика — це голосок у вашій голові, який підказує вам, що правильно, а що ні, направляючи вас ухвалювати правильні рішення. Як фахівець з кібербезпеки, ви повинні розуміти як закон, так і інтереси організації, щоб мати можливість ухвалювати такі рішення.



У 19 столітті філософи Джеремі Бентам і Джон Стюарт Мілл сформулювали теорію утилітарної етики. Теорія базується на принципі, що наслідок дії є найважливішим фактором, щоб визначити моральність чи аморальність вчинку, де етичним вибором є дія, яка максимізує найбільше благо



Правовий підхід керується принципом, який стверджує, що особа має право зробити власний вибір, який не може бути порушений рішенням іншої особи. Це рішення має поважати та враховувати основні права людини. До таких основних прав належать право на правду, право на конфіденційність, право на безпеку



Підхід загального блага пропонує вважати етичними дії, які приносять користь усій громаді. Це провокує людей визнавати та дотримуватися спільних з іншими членами громади цінностей та цілей.

Для фахівця із кібербезпеки часто не існує очевидної відповіді на етичне запитання, що виникло. Правильний напрям дій буде залежати від ситуації та етичного погляду, який ви використовуєте, щоб керувати своїм рішенням.

Інститут комп'ютерної етики (Computer Ethics Institute – CEI), який знаходиться у Вашингтоні, округ Колумбія, є ресурсом для ідентифікації, оцінки та реагування на етичні проблеми у галузі інформаційних технологій. Це була одна з перших організацій, яка визнала етичні проблеми та проблеми публічних політик, що виникають внаслідок швидкого розвитку галузі інформаційних технологій.

Галузеві закони США

Фінанси

Закон Грема-Ліча-Блайлі (Gramm-Leach-Bliley Act – GLBA) – це законодавчий акт, який стосується переважно фінансової галузі. Частина цього закону містить положення, які дозволяють фізичним особам контролювати використання інформації, якою вони поділилися із організацією під час здійснення господарської операції. GLBA обмежує обмін інформацією зі сторонніми фірмами.

Корпоративний облік

Після кількох гучних скандалів навколо корпоративного обліку в США, у 2002 році Конгрес прийняв Закон Сарбейнса-Окслі (Sarbanes-Oxley Act – SOX), щоб переглянути стандарти фінансового та корпоративного обліку. Зокрема, він орієнтувався на фінансові стандарти та практики торговельних фірм відкритого типу у країні.

Кредитні картки

Приватні підприємства також наголошують на важливості уніфікованих та застосовних стандартів, і в 2006 році Рада зі стандартів безпеки, що складається з провідних організацій у галузі платіжних карток, розробила ініціативу приватного сектора для покращення конфіденційності мережних комунікацій.

Стандарт безпеки даних індустрії платіжних карток (Payment Card Industry Data Security Standard – PCI DSS) — це набір договірних правил, які спрямовані на захист платіжних даних власників платіжних карток під час транзакції та зменшення шахрайства. Теоретично PCI DSS є добровільним стандартом. Однак на практиці будь-яка організація, яка зберігає, обробляє або передає дані власника картки, які не відповідають стандарту PCI DSS, може зіткнутися зі значно вищими комісіями за транзакції, штрафами до $500000 і, у виняткових випадках, втратити можливість обробляти платіжні картки.

Криптографія

Організації, які імпортують або експортують комерційні продукти шифрування, підпадають під дію правил, які контролюються Бюро промисловості та безпеки Міністерства торгівлі.

Обмеження на експорт до країн-вигнанців і терористичних організацій можуть бути введені через проблеми національної безпеки.

Крім того, деякі країни можуть вирішити обмежити імпорт криптографічних технологій через побоювання, що:

Технологія містить бекдор або вразливості безпеки.

Громадяни зможуть використовувати цю технологію для анонімного спілкування та уникнути контролю з боку влади.

Рівень конфіденційності може підвищитися вище прийнятного рівня.

Захист конфіденційності громадян США

Закон про конфіденційність (Privacy Act) 1974

Цей закон встановлює кодекс доброчесних інформаційних практик, які регулюють збирання, збереження, використання та поширення федеральними агентствами конфіденційних персональних даних, які зберігаються в системах обліку.

Закон про свободу інформації (Freedom of Information Act — FOIA)

FOIA забезпечує доступ громадськості до урядових документів США. Він передбачає презумпцію розкриття інформації, яка означає, що уряд зобов'язаний вказати вагому причину з якої інформація не може бути оприлюднена.

Є дев'ять винятків щодо розкриття інформації, які стосуються FOIA:

1. Інформація, що стосується національної безпеки та зовнішньої політики
2. Внутрішні правила та інструкції для персоналу організації
3. Інформація, яка спеціально вилучена за законом
4. Конфіденційна комерційна інформація
5. Між- або внутрішньо організаційне спілкування, яке підлягає обговоренню, судовому розгляду та іншим привілеям
6. Інформація, яка, в разі розголошення, становитиме явно необґрунтоване вторгнення в особисте життя
7. Матеріали правоохоронних органів, які стосуються вказаних аспектів
8. Агентська інформація від фінансових установ
9. Геологічна та геофізична інформація про свердловини

Закон про сімейні освітні права та конфіденційність (Family Educational Rights and Privacy Act — FERPA)

Цей федеральний закон регулює доступ до записів про освіту.

Він працює на основі згоди. Це означає, що батьки повинні дати дозвіл на оприлюднення освітньої інформації про учня державним суб'єктам до фактичного оприлюднення цієї інформації. Коли учню виповниться 18 років або він вступить до вищого навчального закладу в будь-якому віці, то ці права, за FERPA, перейдуть від батьків учня до самого учня.

Закон США про захист конфіденційності дітей в Інтернеті (Children's Online Privacy Protection Rule — COPPA)

Цей федеральний закон був створений для захисту конфіденційності дітей віком до 13 років, шляхом встановлення певних вимог до операторів веб-сайтів та онлайн-сервісів під юрисдикцією США. Наприклад, потрібно отримати згоду батьків, перш ніж організація зможе збирати та використовувати інформацію від дітей віком до 13 років.

Оцінка впливу на конфіденційність (Privacy impact assessment — PIA)

PIA – це процес, який допомагає забезпечити належну обробку персональних даних (personally identifiable information — PII) у всій організації.

Дванадцять доменів кібербезпеки

Опубліковані Міжнародною організацією зі стандартизації (International Organization for Standardization – ISO) та Міжнародною електротехнічною комісією (International Electrotechnical Commission – ICO), стандарти ISO 27000 встановлюють вимоги до комплексної системи управління безпекою інформації (information security management system – ISMS). ISMS складається з адміністративних, технічних та операційних засобів контролю інформаційної безпеки в організації.
Стандарт ISO 27000 представлений дванадцятьма незалежними доменами.

Оцінка ризиків
: Перший крок у процесі управління ризиками, який передбачає кількісне та якісне вимірювання ризику конкретної ситуації чи загрози.

Політика безпеки
: У цьому документі розглядаються обмеження та дії співробітників в організації, а також часто вказується, як і хто може отримати доступ до даних.

Організація інформаційної безпеки
: Це модель управління інформаційною безпекою, що впроваджена організацією.

Управління активами
: Це схема проведення інвентаризації та класифікації інформаційних активів в організації.

Безпека людських ресурсів
: Стосується процедур безпеки, що пов'язані із прийняттям, переміщення всередині організації та звільненням працівників.

Фізична безпека та безпека середовища
: Стосується фізичного захисту об’єктів та інформації в організації.

Комунікаційний та операційний менеджмент
: Стосується управління технічними засобами контролю безпеки систем і мереж організації.

Придбання, розробка та обслуговування інформаційних систем
: Стосується безпеки як невід’ємної частини інформаційних систем організації.

Контроль доступу
: Описує, як організація обмежує права доступу до мереж, систем, функцій програм і даних, щоб запобігти несанкціонованому доступу користувачів.

Керування подіями інформаційної безпеки
: Описує організаційний підхід до прогнозування та реагування на порушення інформаційної безпеки.

Керування безперервністю бізнесу

Відповідність

Цілі та засоби контролю

Ці дванадцять доменів складаються з цілей контролю (ISO 27001) і засобів контролю (ISO 27002).



Цілі контролю визначають високорівневі вимоги для впровадження комплексної системи управління інформаційною безпекою в організації і, зазвичай, надають контрольний список, який використовується під час аудиту ISMS.
Проходження цього аудиту свідчить про те, що організація відповідає стандарту ISO 27001 і запевняє партнерів у безпечності даних та операцій організації.



Елементи контролю показують, як досягти цілей контролю в організації. Вони надають рекомендації щодо впровадження, підтримки та покращення управління інформаційною безпекою в організації.

ISO 27000 є універсальною концепцією для організації будь-якого типу. Щоб ефективно використовувати концепцію у своєму середовищі та у своїй діяльності організація повинна визначити сфери, цілі контролю та засоби контролю.
Для цього, більшість організацій формують заяву про застосовність (statement of applicability – SOA), яка дозволяє адаптувати доступні цілі та засоби контролю, щоб якнайкраще відповідати встановленим пріоритетам щодо конфіденційності (confidentiality), цілісності (integrity) та доступності (availability) – тріада CIA.

Засоби контролю ISO орієнтовані на забезпечення безпеки даних у будь-якому з трьох станів: в обробці, у стані спокою (зберігання) та у транзитному стані (передавання).
Відповідальність за визначення та впровадження відповідних засобів контролю можуть нести різні групи в організації.

Матриця керування хмарою

Альянс хмарної безпеки (Cloud Security Alliance – CSA) надає рекомендації з безпеки будь-якій організації, яка використовує хмарні обчислення, або прагне оцінити загальний ризик безпеки постачальника хмарних послуг. Розроблена ними матриця контролю хмари (Cloud Controls Matrix – CCM) увідповіднює спеціальні засоби контролю безпеки у хмарі з провідними стандартами, найкращими практиками та правилами. Вона складається із 197 цілей контролю, які структуровано у 17 областях, що охоплюють усі аспекти хмарних технологій, включаючи управління та ризики, людські ресурси та безпеку мобільних пристроїв.
CCM вважається де-факто стандартом для забезпечення безпеки та відповідності в хмарі.

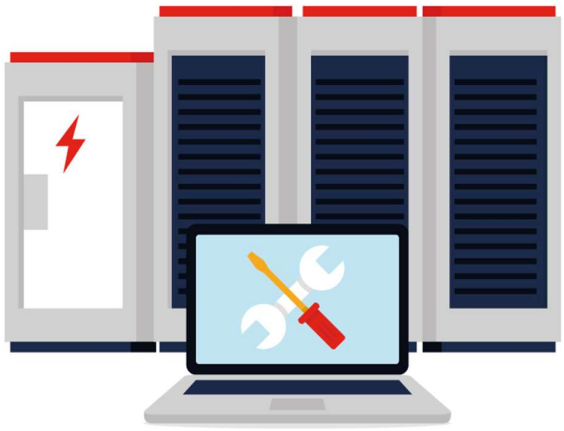


Відповідність

Постачальникам послуг може знадобитися надання гарантій своїм організаціям-клієнтам, що впроваджені ними засоби контролю безпеки розроблені належним чином та ефективно виконуються.

Утиліти діагностики для командного рядка

Існує сукупність інструментів командного рядка, які можна використовувати для оцінки позиції безпеки



- ipconfig відображає налаштування TCP/IP (IP-адреса, маска підмережі, шлюз за замовчуванням, інформація про DNS і MAC (*ifconfig* є еквівалентом для Mac/Linux).
- ping перевіряє мережне підключення, надсилаючи ICMP запит на хост і визначає, чи доступний маршрут для хоста.
- arp надає таблицю, яка зіставляє відомі MAC-адреси з пов'язаними з ними IP-адресами, і є швидким способом знайти MAC-адресу кінцевого пристрою.
- tracert відстежує маршрут, яким проходить пакет до місця призначення, і записує пристрої на цьому шляху, допомагаючи визначити місця зависання пакету (*traceroute* є еквівалентом для Mac/Linux).
- nslookup запитує DNS-сервер, щоб допомогти усунути неполадки з базою даних DNS (*dig* є еквівалентом для Mac/Linux).
- netstat відображає всі порти, які комп'ютер прослуховує, і може визначити активні з'єднання.
- nbtstat допомагає усунути проблеми з визначенням імен NetBIOS в системі Windows.
- nmap використовується в аудиті безпеки. Визначає місцезнаходження мережних хостів, виявляє операційні системи та ідентифікує служби.
- netcat збирає інформацію з мережних з'єднань TCP і UDP, а також може використовуватися для сканування портів, моніторингу, захоплення банерів і копіювання файлів.
- hping збирає та аналізує пакети і використовується для сканування портів, прокладання маршрутів, ідентифікації ОС і тестування брандмауера.

Автоматизація безпеки

Давайте тепер розглянемо деяку інформацію про автоматизовані підходи до управління інформацією та подіями безпеки (Security Information and Event Management – SIEM) та автоматизації оркестрації безпеки і реагування (Security Orchestration Automation and Response – SOAR).

SIEM

Системи управління інформацією та подіями безпеки (Security Information and Event Management – SIEM) збирають дані із пристроїв безпеки, мережних пристроїв, серверів та програм для представлення цих даних у журналах. Журнали можуть генерувати багато подій протягом дня, тому системи SIEM допомагають зменшити обсяг подій, поєднуючи подібні події, щоб зменшити навантаження на дані про події. SIEM визначає відхилення від норми, а потім вживає відповідні заходи.

Цілями системи SIEM під час моніторингу безпеки є:
Визначення будь-яких внутрішніх та зовнішніх загроз
Відстеження активності та використання ресурсів
Створення звітів про відповідність для аудитів
Підтримка реагування на інцидент

Коли система SIEM виявляє потенційну проблему, вона може записувати додаткову інформацію, генерувати сповіщення та рекомендувати іншим елементам керування безпекою припинити діяльність. Розширені системи SIEM аналізують поведінку користувачів і сутностей, які шукають моделі, що залежать від людських настроїв, щоб розпізнати загрозу, перш ніж вона стане реальною.
Обсяг даних, які реєструються з критично важливих систем, є важливим фактором при впровадженні системи SIEM, оскільки вам потрібно буде переглядати створені звіти. Придбання та обслуговування систем SIEM є дороговартісним, а рентабельні вони лише тоді, коли в організації протягом дня генеруються мільйони подій.

SOAR

Інструменти автоматизації оркестрації безпеки і реагування (Orchestration Automation and Response – SOAR) дозволяють організації збирати дані про загрози безпеці з різних джерел і реагувати на події низького рівня без втручання людини. SOAR має три важливі функції:
Управління загрозами та вразливостями
Реагування на інциденти
Автоматизація операцій з безпеки
Організація може інтегрувати SOAR у своє SIEM рішення.

Інструменти тестування мережі

Існує багато інструментів для перевірки безпеки систем і мереж. Деякі з цих інструментів є інструментами із відкритим кодом, а інші – комерційними інструментами, які потребують придбання ліцензії на використання.
Для тестування мережі можна використовувати такі програмні засоби:

- Nmap/Zenmap – це програмне забезпечення для виявлення комп'ютерів та їхніх служб у мережі, створюючи таким чином карту мережі.
- SuperScan – це програмне забезпечення для сканування портів, розроблене для виявлення відкритих портів TCP і UDP, визначення служб, які працюють на цих портах, а також для виконання запитів, таких як whois, ping, traceroute, та пошуку імен хостів.
- Система управління інформацією та подіями безпеки (Security Information Event Management – SIEM) – це технологія, яка використовується корпораціями для надання звітів у реальному часі та для довгострокового аналізу подій безпеки.
- GFI LANguard – це сканер мережі та безпеки, який виявляє вразливості.
- Tripwire – це інструмент для оцінювання та перевірки IT-конфігурації на відповідність внутрішнім політикам, стандартам відповідності та найкращим практикам безпеки.
- Nessus – це програмне забезпечення для сканування вразливостей, що орієнтовано на віддалений доступ, некоректні конфігурації і DoS стеку TCP/IP.
- L0phtCrack – це програмний додаток для перевірки та відновлення паролів.
- Metasploit – це засіб, який надає інформацію про вразливості, допомагає проводити тестування на проникнення та розробляти IDS сигнатуру.

Тестування на проникнення

- Тестування методом чорної скриньки є найшвидшим та найдешевшим методом тестування. Тестуючи методом чорної скриньки, фахівець нічого не знає про внутрішню роботу системи і намагається атакувати її як звичайний користувач.

- Тестування методом сірої скриньки це тестування, в якому поєднано тестування методом «чорної скриньки» та тестування методом білої скриньки. Фахівець має деякі обмежені знання про систему, тому це частково відоме середовище, що надає певну перевагу цій спробі злому.

- Тестування методом білої скриньки є найтривалішим та найдорожчим, оскільки виконується фахівцем, який знає, яким чином працює система. Це відоме середовище, в якому здійснюються спроби зламу, імітуючи зловмисну атаку інсайдера або того, кому вдалося отримати таку інформацію заздалегідь на етапі розвідки.

Спільноти з мережної аналітики

Щоб бути ефективним, фахівець із мережної безпеки повинен:

- Знати про останні кіберзагрози – новини в режимі реального часу щодо кіберзагроз, регулярно переглядати веб-сайти, пов'язані із безпекою, переглядати блоги з кібербезпеки та подкасти, тощо.
- Продовжувати вдосконалювати навички – регулярно відвідувати тренінги з кібербезпеки, семінари та конференції.

Організація	Опис
SANS	Ресурси SysAdmin, Audit, Network, Security Institute(SANS) здебільшого безкоштовні і включають: • Центр моніторингу мережних загроз (Internet Storm Center) – популярна система раннього попередження в Інтернеті. • NewsBites – щотижневий дайджест статей про комп'ютерну безпеку. • @RISK – щотижневий дайджест нещодавно виявлених векторів атак, вразливостей із активними експлоїтами та пояснень того, як працювали останні атаки. • Миттєві сповіщення безпеки. SANS також розробляє курси з безпеки.
Mitre	Корпорація Mitre підтримує перелік поширених вразливостей та ризиків: common vulnerabilities and exposures – CVE
FIRST	Forum of Incident Response and Security Teams (FIRST) – це організація з безпеки, яка об'єднує різні групи реагування на інциденти комп'ютерної безпеки з урядових, комерційних і освітніх організацій для сприяння співпраці та координації обміну інформацією, запобігання інцидентам і швидкого реагування.
SecurityNewsWire	Портал новин безпеки, який збирає останні новини, що стосуються сповіщень, експлоітів і вразливостей.
ISC^2	Міжнародний консорціум із сертифікації безпеки інформаційних систем (International Information Systems Security Certification Consortium – ISC2) – це організація з мережної безпеки, яка надає нейтральні освітні продукти і послуги професійного розвитку
CIS	Center for Internet Security (CIS) є центром запобігання кіберзагрозам, захисту, реагування та відновлення для державних, місцевих, племінних і територіальних (state, local, tribal, and territorial – SLTT) органів влади через Загальнодержавний центр обміну та аналізу інформації (Multi-State Information Sharing and Analysis Center – MS-ISAC).

FireEye

FireEye – це компанія з кібербезпеки, послуги якої допомагають підприємствам захистити свої мережі. FireEye використовує тристоронній підхід, що поєднує аналітику кібербезпеки, експертизу та технології безпеки.

FireEye пропонує SIEM і SOAR з платформою Helix Security Platform, яка використовує поведінковий аналіз і розширене виявлення загроз та підтримується всесвітньою мережею аналітики загроз FireEye Mandiant. Helix — це хмарна безпекова платформа, яка поєднує в собі різноманітні засоби аналітики з кібербезпеки та інструменти безпеки.
Система безпеки FireEye блокує атаки на веб-сайти та електронну пошту через вектори загроз та приховане зловмисне програмне забезпечення, яке знаходиться у файлах, що розповсюджуються. Вона блокує роботу вдосконалених зловмисних програм, які легко обходять традиційні захисти на основі сигнатур і компрометують більшість корпоративних мереж. Ця система не використовує механізм сигнатур і може працювати на всіх стадіях життєвого циклу атаки, використовуючи аналіз стану атаки для виявлення загроз нульового дня.

Автоматизований обмін індикаторами (Automated Indicator Sharing – AIS)

Міністерство національної безпеки Сполучених Штатів Америки (Department of Homeland Security – DHS) пропонує безкоштовний сервіс під назвою «Автоматизований обмін індикаторами» (Automated Indicator Sharing – AIS). AIS у режимі реального часу забезпечує обмін індикаторами кіберзагроз (наприклад, зловмисними IP-адресами, адресами відправників фішингових email-повідомлень та ін.) між Федеральним Урядом США та приватним сектором.
AIS створює екосистему технічних партнерів там, де виявляють загрозу, й інформація про неї поширюється всередині спільноти, щоб допомогти її учасникам захистити власні мережі від конкретної небезпеки.

База даних популярних вразливостей і ризиків (CVE)

Уряд Сполучених Штатів спонсорує корпорацію MITRE з метою створення та ведення каталогу відомих вразливостей безпеки, який називається «Типові вразливості та ризики» (Common Vulnerabilities and Exposures – CVE). CVE виконує функції словника загальноприйнятих назв (так званих ідентифікаторів CVE) для відомих вразливостей кібербезпеки.
Щоб спростити обмін даними корпорація MITRE визначає унікальні ідентифікатори CVE для відомих вразливостей, пов'язаних з інформаційною безпекою.

Стандарти обміну даними для аналізу кіберзагроз

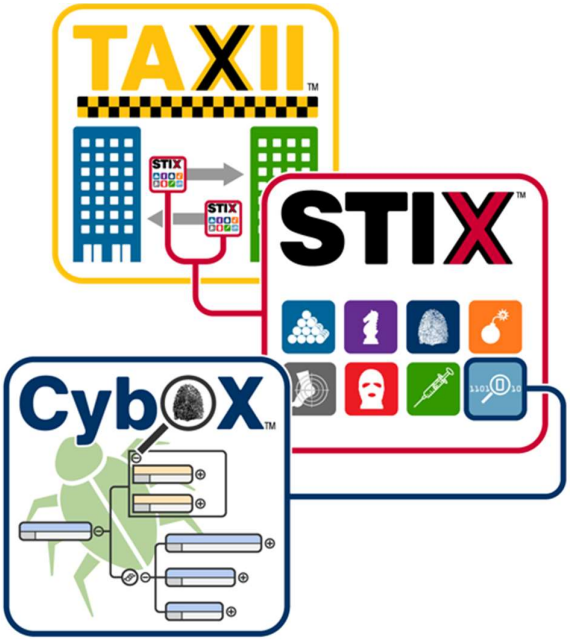
Мережним Організаціям та фахівцям необхідно обмінюватися інформацією для підвищення рівня знань про зловмисників, а також про ресурси, до яких вони бажають отримати доступ. З метою забезпечення зв'язку між багатьма мережними платформами було розроблено кілька відкритих стандартів обміну аналітичною інформацією. Ці стандарти дозволяють здійснювати обмін інформацією про аналіз кіберзагроз (cyber threat intelligence – CTI) у автоматичному, узгодженому форматі, придатному для машинної обробки. Є три загальноприйняті стандарти для обміну інформацією про аналіз загроз:

- Структуроване подання інформації про загрози (Structured Threat Information Expression – STIX) – це сукупність специфікацій для обміну інформацією про кіберзагрози між Організаціями. Стандарт відкритих виразів (Cyber Observable Expression – CybOX) було додано до STIX.

- Надійний автоматизований обмін інформацією про показники (Trusted Automated Exchange of Indicator Information – TAXII) – це специфікація протоколу прикладного рівня, що дозволяє передавати CTI через HTTPS. Стандарт TAXII створений для підтримки стандарту STIX.

- CybOX – це стандартизована схема, призначена для визначення, фіксації, характеристики та передавання подій і властивостей про мережні операції, а також підтримки багатьох інший функцій кібербезпеки.

Ці відкриті стандарти містять специфікації, які сприяють автоматичному обміну інформацією про кіберзагрози у стандартизованому форматі.



Платформа для обміну інформацією про зловмисне програмне забезпечення (Malware Information Sharing Platform – MISP) є відкритою платформою для обміну індикаторами компрометації для нещодавно виявлених загроз. MISP підтримується Європейським Союзом і використовується у більш ніж 6000 організацій по всьому світу. MISP дозволяє автоматизувати обмін IOC між людьми та машинами за допомогою STIX та інших форматів експорту.

Профілювання мережі

Для виявлення серйозних інцидентів безпеки важливо зрозуміти, охарактеризувати та проаналізувати інформацію про нормальне функціонування мережі.

Елемент мережного профілю	Опис
Тривалість сесії	Це час від встановлення з'єднання для передавання потоку даних до його припинення.
Загальна пропускна здатність	Це сумарна кількість даних, що передаються від деякого джерела до заданого пункту призначення за певний період часу.
Використані порти	Це перелік процесів TCP або UDP, що доступні для одержання даних.
Адресний простір ресурсів	Це IP-адреси або логічне розташування важливих систем чи даних.

Профілювання сервера

Профілювання сервера використовується для встановлення прийнятного робочого стану серверів. Профіль сервера – це базовий рівень безпеки для даного сервера, що встановлює параметри мережі, користувача та програми.

Для того, щоб створити профіль сервера, важливо зрозуміти функцію, яку сервер має виконувати в мережі. Звідси різні параметри керування та використання можуть бути визначені та задокументовані.

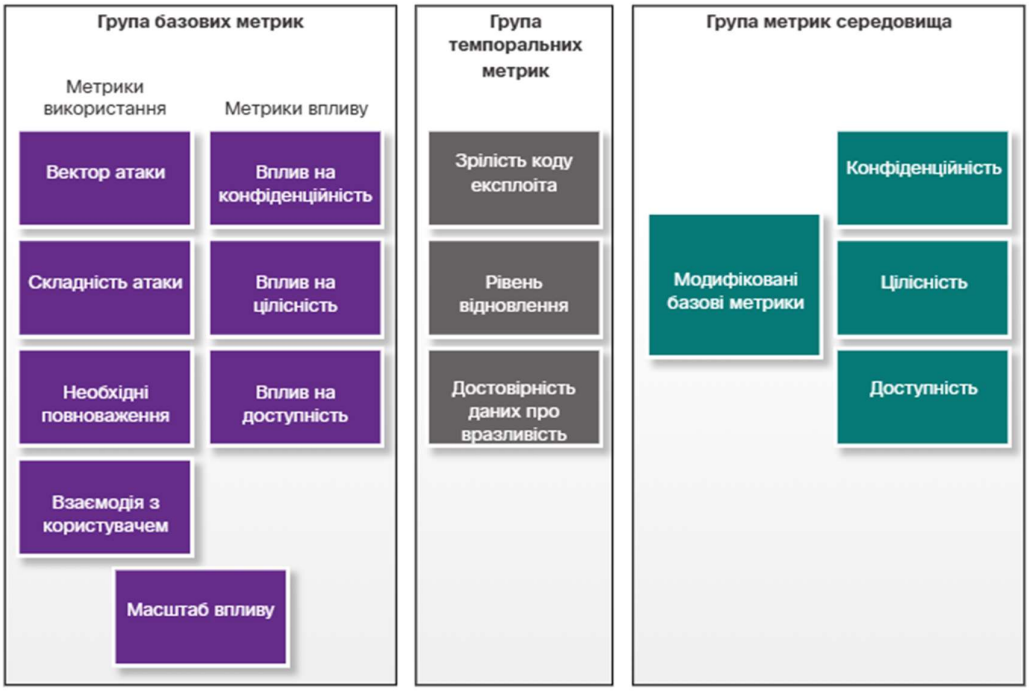
Елемент мережного профілю	Опис
Відкриті порти	Це TCP і UDP демони та порти, які зазвичай можуть бути відкриті на сервері.
Облікові записи користувачів	Це параметри, що визначають доступ і поведінку користувача.
Облікові записи служб	Це визначення типу функції, яку програмі дозволено виконувати на даному хості.
Програмне середовище	Це завдання, процеси та програми, які дозволено запускати на сервері.

Огляд CVSS

Common Vulnerability Scoring System (CVSS) – це інструмент для оцінювання ризику, що розроблений для передачі загальних атрибутів та ступеня серйозності вразливостей в апаратних та програмних комп'ютерних системах. Третя редакція, CVSS 3.0, є нейтральним і відкритим галузевим стандартом для встановлення пріоритетності ризиків вразливостей з використанням різних метрик.

Групи метрик CVSS

Перш ніж проводити оцінку CVSS, важливо вивчити основні Терміни, які використовуються в інструменті оцінки. Багато метрик враховують роль того, що в CVSS називається уповноваженою сутністю.



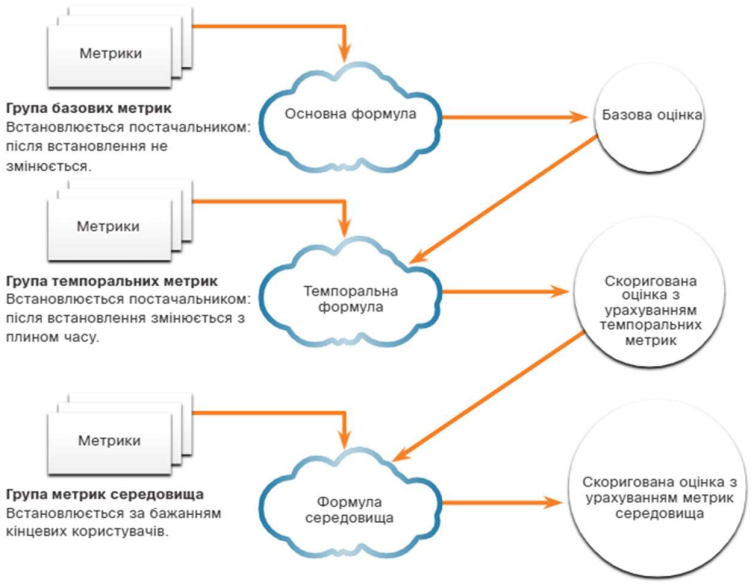
Звіти CVSS

Рейтинг серйозності	Значення CVSS
Відсутній	0
Низький	0.1-3.9
Середній	4.0-6.9
Високий	7.0-8.9
Критичний	9.0-10.0

Процес CVSS

У таблиці наведено розшифровку для групи базових показників.

Назва метрики	Позначення	Можливі значення	Значення
Вектор атаки	AV	[N, A, L, P]	N = Мережний A = Суміжній L = Локальний P = Фізичний
Складність атаки	AC	[L, H]	L = Низька H = Висока
Необхідні повноваження	PR	[N, L, H]	N = Відсутні L = Низькі H = Високі
Взаємодія з користувачем	UI	[N, R]	N = Відсутня R = Необхідна
Масштаб впливу	S	[U, C]	U = Незмінний C = Змінюваний
Вплив на конфіденційність	C	[H, L, N]	H = Високий L = Низький N = Відсутній
Вплив на цілісність	I	[H, L, N]	H = Високий L = Низький N = Відсутній
Вплив на доступність	A	[H, L, N]	H = Високий L = Низький N = Відсутній



Процес управління ризиками

Ризик – це ймовірність втрати через загрозу – зловмисну дію чи несподівану подію – яка завдає шкоди інформаційним системам або активам організації.

Управління ризиками – це формальний процес, який вимірює вплив загрози та витрати на впровадження засобів контролю або контрзаходів для зниження цієї загрози. Ризик неможливо повністю усунути, але його все одно можна знизити до прийнятного рівня.



Окреслення ризику

Передбачає визначення загроз в організації, які підвищують ризик. Виявлені загрози включають втрату або пошкодження процесів і продуктів, атаки, потенційний збій або порушення роботи сервісів, завдання шкоди репутації організації, юридичну відповідальність та втрату інтелектуальної власності.



Оцінка ризику

Після визначення ризику його оцінюють та аналізують, щоб визначити серйозність загрози. Деякі загрози можуть призвести до простою всієї організації, тоді як інші загрози є лише незначними незручностями. Ризику може бути встановлено пріоритет за фактичним фінансовим впливом (кількісний аналіз) або масштабованим впливом на діяльність організації (якісний аналіз).

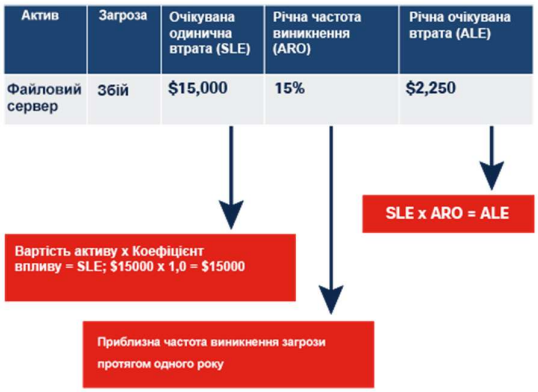


Відповідь на ризик

Передбачає розробку плану дій для зменшення впливу ризику на організацію загалом. Керівництво оцінює загрози та визначає їх пріоритети; потім команда визначає, як реагувати на кожну загрозу. Ризик може бути усунутий, знижений, переданий або прийнятий.

Кількісний аналіз ризиків

Кількісний аналіз ризиків присвоює числа процесу аналізу ризиків. У прикладі, вартість активу є вартістю заміни файлового сервера (активу). Вартість активу також може бути виміряна доходами, отриманими за рахунок використання активу.



Коефіцієнт впливу (exposure factor) – це суб'єктивне значення, виражене у відсотках втрати файлового сервера через конкретну загрозу. Якщо відбувається повна втрата, EF дорівнює 1,0 (100%).

Річна частота виникнення (annualized rate of occurrence) – це ймовірність того, що втрата виникне протягом року. Показник ARO може перевищувати 100%, якщо втрата траплятиметься частіше одного разу на рік.

Якісний аналіз ризиків

Якісний аналіз ризику використовує оцінки та сценарії, які відображають відношення ймовірності виникнення загрози до її впливу. У прикладі, збій сервера є ймовірним, але його вплив може бути незначним.
Матриця ризиків – це інструмент, який допомагає визначити пріоритети ризиків, щоб визначити, на які з них організація має розробити відповідь.

Категорія	Часто - 5	Ймовірно - 4	Зрідка - 3	Рідко - 2	Малоймовірно - 1
Катастрофічний - 4	20	16	12	8	4
Критичний - 3	15	12	9	6	3
Граничний - 2	10	8*	6	4	2
Незначний - 1	5	4	3	2	1

* Збій сервера

Типи контролю

Адміністративний контроль складається з процедур і політик, які організація встановлює коли має справу з конфіденційною інформацією.

Технічний контроль охоплює апаратне та/або програмне забезпечення, впроваджене для управління ризиками та забезпечення захисту.

Фізичний контроль – це механізми, такі як огорожі та замки, що використовуються для захисту систем, об’єктів, персоналу та ресурсів. Фізичний контроль фізично відокремлює людей або інші загрози від систем.