Принципи, практики, процеси захисту мережі

Аналітик з кібербезпеки повинен бути готовим до будь-якого типу атак. Його робота полягає у захисті активів мережі організації. Для цього аналітик з кібербезпеки повинен спершу визначити:

- **Активи** – все, що становить цінність для організації та потребує захисту, зокрема, сервери, пристрої мережної інфраструктури, кінцеві вузли та, як найголовніший ресурс, дані.
- **Вразливості** – це слабкі місця в системі або в її конструкції, якими може скористатися зловмисник.
- **Загрози** – будь-яка потенційна небезпека для активу.

Класифікація активів

Класифікація активів дозволяє згрупувати всі ресурси організації за деякими спільними характеристиками. Найбільш важлива інформація потребує забезпечення найвищого рівня захисту та навіть може вимагати спеціальної обробки.

Крок 1

Визначте відповідну категорію ідентифікації активів:

- Інформаційні активи
- Програмні активи
- Фізичні активи
- Служби

Крок 2

Встановіть відповідальність за активи, визначивши власника кожного інформаційного активу та кожного програмного засобу:

- Визначте власника всіх інформаційних активів.
- Визначте власника програмного забезпечення усіх застосунків.

Крок 3

Визначте критерії класифікації:

- Конфіденційність
- Вартість
- Час
- Права доступу
- Знищення

Крок 4

Реалізуйте систему класифікації:

- Використовуйте єдиний спосіб ідентифікації інформації, який би забезпечив уніфікований захист та спрощений моніторинг.

Визначення вразливостей

При виявленні загроз важливо поставити декілька запитань:

- Які можливі вразливості системи?
- Хто може скористатися цими вразливості для доступу до конкретних інформаційних активів?
- Які наслідки використання цих вразливостей та втрати активів?



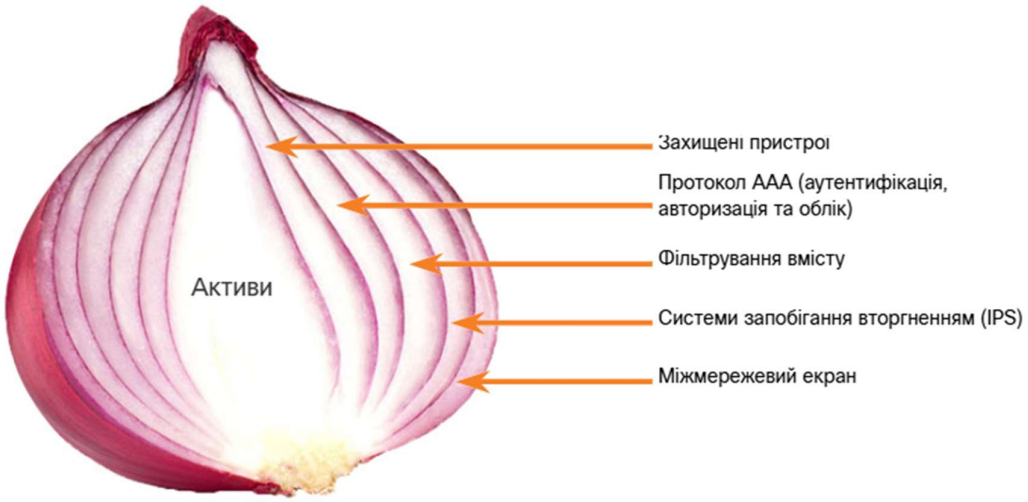
До найбільш поширених загроз банківській електронній системі належать:

- **Несанкціонований доступ до внутрішньої системи** – Нападник використовує відкриті сервери електронного банкінгу для втручання до внутрішньої банківської системи.
- **Крадіжка клієнтських даних** – Зловмисник викрадає персональну та фінансову інформацію банківських клієнтів з бази даних користувачів.
- **Шахрайські транзакції з зовнішнього сервера** – Нападник змінює код програми електронного банкінгу і виконує транзакції від імені законного користувача.
- **Підроблені транзакції з використанням викраденого PIN-коду або смарт-карти клієнта** – Зловмисник викрадає ідентифікаційні дані клієнта і здійснює зловмисні транзакції зі скомпрометованого рахунку.
- **Внутрішня атака на систему** – Банківський працівник виявляє у системі недолік, яким можна скористатися для проведення атаки.
- **Помилки введення даних** – Користувач вводить некоректні дані або формує неправильні запити на виконання транзакцій.

Захист за принципом цибулі та артишоку

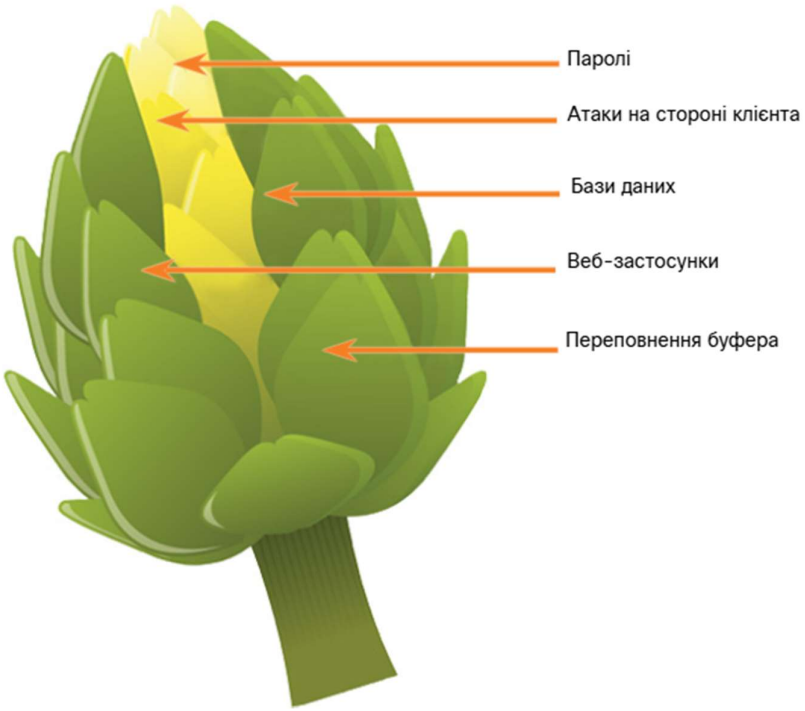
Security Onion

Поширена аналогія, що використовується для опису підходу глибинної оборони має назву "security onion"



Захист за принципом артишоку

Як показано на рисунку, зловмисникам достатньо зняти лише потрібні "листки артишоку", де кожен "листок" мережі може розкривати дані



Методи написання коду, що сприяють безпеці

Нормалізація

Нормалізація використовується для організації даних у базі даних та підтримки їх цілісності. Завдяки нормалізації вхідний рядок можна звести до найпростішої з відомих форм, яка забезпечує усім рядкам унікальне двійкове подання, та можливість виявити введення будь-яких шкідливих даних.

Збережена процедура

Збережена процедура — це група попередньо скомпільованих операторів SQL, що зберігаються у базі даних та виконують деяку дію. Застосування збереженої процедури для отримання вхідних параметрів від клієнтів, що використовують різні вхідні дані, сприятиме зменшенню мережного трафіку та швидшому одержанню результатів.

Обфускація та камуфляж

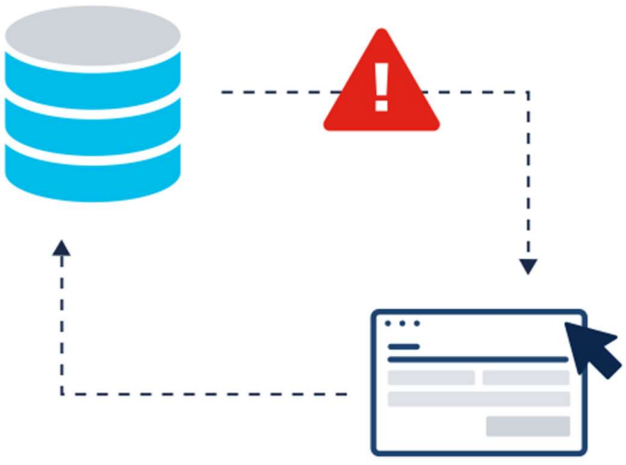
Розробник може використовувати обфускацію (затуманювання) та камуфляж щоб запобігти зворотному проектуванню програмного забезпечення (reverse engineering). Обфускація приховує вихідні дані за допомогою випадкових символів або даних. Камуфляж замінює конфіденційні дані на вигадані, що дуже подібні до реальних.

Повторне використання коду

Повторне використання коду означає залучення наявного програмного забезпечення для створення нової програми, з метою заощадження часу та зусиль на розробку. Однак, це потрібно робити з обережністю, аби уникнути введення вразливостей.

Пакети SDK

Сторонні бібліотеки та комплекти для розробки програмного забезпечення (software development kits, SDK), як сховища корисного коду, роблять розробку застосунків швидшою та дешевшою. Недоліком є те, що будь-які вразливості в SDK або сторонніх бібліотеках потенційно можуть поширитися на багато програм.



Контроль процесу введення даних є ключовим для підтримки цілісності баз даних. Саме проти них запускають велику кількість атак, які, зокрема, засновані на впровадженні спотворених даних.

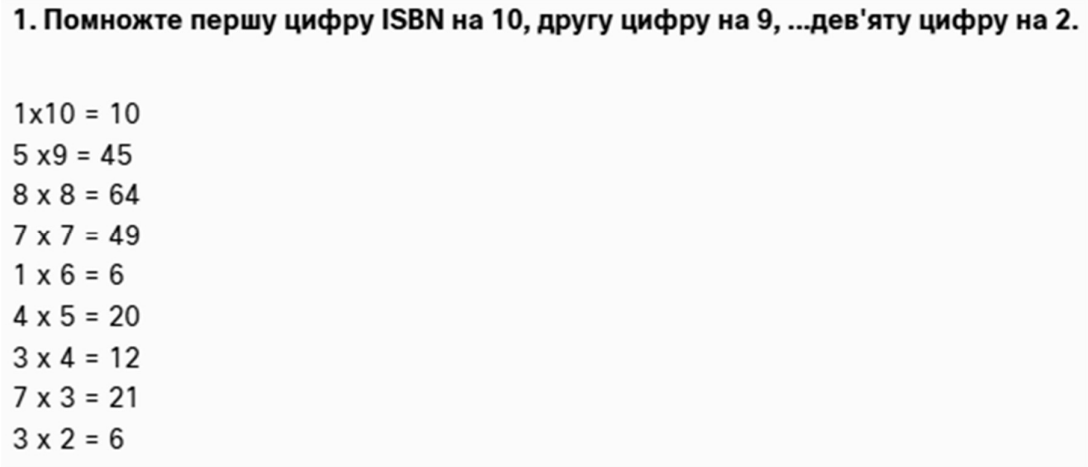
Правила перевірки

Правило валідації перевіряє, чи відповідають дані параметрам, визначеним при проектуванні бази даних. Правило валідації допомагає забезпечити повноту, точність і узгодженість даних

- Розмір - перевіряє кількість символів в елементі даних
- Формат - перевіряє, чи відповідають дані вказаному формату
- Узгодженість - перевіряє узгодженості кодів у відповідних елементах даних
- Діапазон - перевіряє, чи дані перебувають у межах визначеного діапазону
- Контрольна цифра - використовує додаткові обчислення для створення контрольної суми, призначеної для виявлення помилок



1. Помножте першу цифру ISBN на 10, другу цифру на 9, ...дев'яту цифру на 2



2. Додайте всі числа.

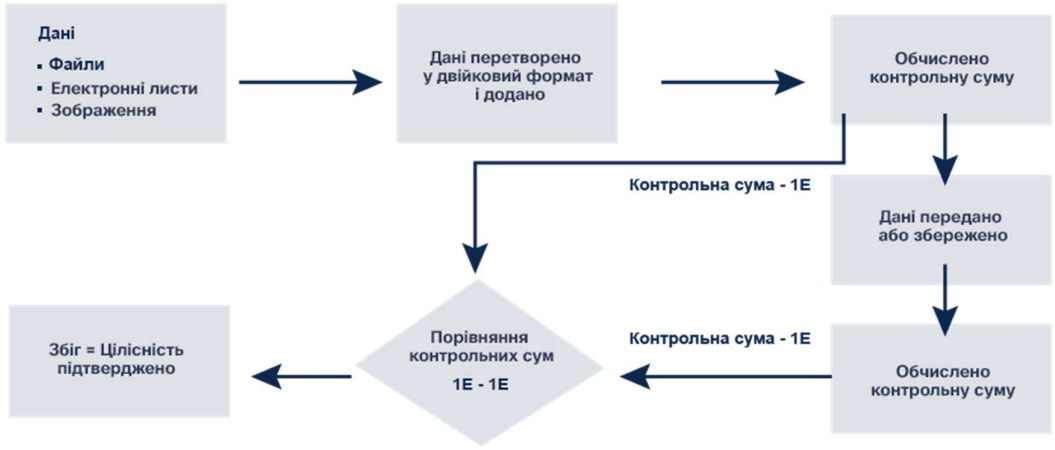
10 + 45 + 64 + 49 + 6 + 20 + 12 + 21 + 6 = 233

3. Контрольна цифра - це число, яке необхідно додати до одержаної суми, щоб вона була кратною 11.

Додайте 9 до 233, щоб одержати число 242, кратне 11

Перевірка цілісності

Скомпрометовані дані можуть загрожувати безпеці ваших пристроїв та систем.
Перевірка цілісності дозволяє оцінити узгодженість даних у файлі, зображенні або записі, аби запевнитись, що вони не були пошкоджені. Перевірка цілісності виконується за допомогою хеш-функції, яка створює відбиток даних, за яким далі можна переконатися, що дані залишилися незмінними. Прикладом застосування хеш-функції є контрольна сума.



Як працює контрольна сума

Контрольна сума перетворює кожну частину інформації в значення і визначає їх загальну суму. Щоб перевірити цілісність даних, система, до якої надходить файл, повторює цей процес. Якщо дві суми збігаються, дані дійсні. Якщо ні, десь під час передавання відбулися зміни.

Хеш-функції

До найбільш поширених хеш-функцій належать MD5, SHA-1, SHA-256 і SHA-512. Вони використовують складні математичні алгоритми для порівняння даних із хешованим значенням. Наприклад, після завантаження користувач може перевірити цілісність файлу, порівнюючи хеш-значення джерела з тим, яке можна згенерувати за допомогою будь-якого калькулятора хешу.

Контроль версій

Організації використовують контроль версій для запобігання випадковим змінам, які можуть вносити уповноважені користувачі. Контроль версій означає, що два користувачі не можуть одночасно оновлювати один і той самий об’єкт, як-от, файл, запис у базі даних або транзакцію.

Авторизація

Авторизація визначає, хто має доступ до ресурсів організації, виходячи з необхідності.

Мережні служби та послуги маршрутизації

Кіберзлочинці використовують вразливі мережні служби як для нападу на пристрій, так і для залучення його до інших атак. Перевірити наявність ненадійних мережних сервісів можна за допомогою сканера для пошуку відкритих портів на пристрої.

Протокол динамічного налаштування вузла (DHCP)

У своїй роботі протокол DHCP (Протокол динамічного налаштування вузла) використовує сервер для автоматичного призначення IP-адрес та інших параметрів конфігурації мережним пристроям. Фактично, пристрій отримує від DHCP-сервера дозвіл на використання мережної інфраструктури.

Система доменних імен (DNS)

DNS (Система доменних імен) перетворює URL-адресу або адресу веб-сайту, як-от, www.cisco.com, на числову IP-адресу. Щоразу, коли користувачі в адресному рядку вводять веб-адресу, DNS-сервер визначатиме відповідну їй IP-адресу. Зловмисники можуть атакувати DNS-сервери, щоб заборонити доступ до мережних ресурсів або перенаправляти трафік на шахрайські веб-сайти.

Протокол міжмережних керуючих повідомлень (ICMP)

Мережні пристрої використовують ICMP (Протокол міжмережних керуючих повідомлень) для надсилання повідомлень про помилки, наприклад, якщо запитувана служба недоступна або хосту не вдалося зв'язатися з маршрутизатором.

Команда ping - це мережна утиліта, яка використовує ICMP для перевірки доступності вузла в мережі.

Протокол маршрутної інформації (RIP)

RIP (Протокол маршрутної інформації) - це протокол маршрутизації, який обмежує у мережі кількість пересилань, дозволених на шляху від джерела до отримувача. Максимальна кількість стрибків, доступних за протоколом RIP, становить 15. RIP - це протокол маршрутизації, який використовується для обміну даними про маршрути, зокрема, про те, які мережі досяжні з кожного маршрутизатора, і як далеко вони розташовані.

Протокол мережного часу (NTP)

Важливо, щоб у всіх мережах був встановлений правильний час. Правильні часові мітки допоможуть точно відстежувати різні події в мережі, зокрема, порушення безпеки. Крім того, синхронізація часу має вирішальне значення для правильної інтерпретації подій у файлах системного журналу syslog, а також при перевірці цифрових сертифікатів.

RAID

Резервний масив незалежних дисків (Redundant Array of Independent Disks, RAID) може бути апаратним або програмним. Для апаратного рішення потрібен спеціальний апаратний контролер в системі, яка містить RAID-диски. Водночас програмною версією RAID керує програмна утиліта в ОС.

- **Дзеркалювання** — зберігає дані, після чого створює їх дублікат, який зберігає на другому диску.
- **Чередування** — записує дані на кілька дисків, щоб послідовні сегменти зберігалися на різних накопичувачах.
- **Паралелізм** — більш точне попарне чередування. Після чередування генеруються контрольні суми для перевірки відсутності помилок у розподілених даних. Ці контрольні суми зберігаються на третьому диску.

Порівняння рівнів RAID

Рівень RAID	Мін. к-ть дисків	опис	Переваги	Недоліки
0	2	Чередування даних без надмірності	Найвища продуктивність	Немає захисту даних, відмова одного диску призводить до втрати усіх даних
1	2	Дзеркалювання диску	Найвища продуктивність, високий рівень захисту даних оскільки всі дані дублюються	Висока вартість впровадження, оскільки потрібен додатковий накопичувач такого ж або більшого обсягу
2	2	Кодування з виправленням помилок	Цей рівень більше не використовується	Така ж продуктивність може бути досягнута за менших витрат за допомогою RAID 3
3	3	Чередування даних на рівні байтів з дубльованою парністю	Для більших послідовних запитів даних	Не підтримує декілька одночасних запитів на читання та запис
4	3	Чередування даних на рівні блоків з дубльованою парністю	Підтримує декілька одночасних запитів на читання, у разі відмови для заміни одного диску використовується диск-дублікат	Запити на запис є вузькими місцями до виділеного диска парності
5	3	Поєднання чередування та парності даних	Підтримує декілька одночасних операцій читання та запису; Дані записуються на всі диски	Продуктивність запису нижча ніж у RAID 0 і 1

RAID приймає дані, які зазвичай зберігаються на одному диску і поширює їх ще на декілька дисків. Окрім RAID 0, якщо якийсь один диск відмовляє, користувач може відновити дані з інших дисків, на яких вони також зберігаються.
До того ж RAID дає змогу збільшити швидкість відновлення даних, оскільки на кількох дисках швидше віднайти ті самі дані, аніж на одному накопичувачі.

Резервування покращує доступність інфраструктури, захищаючи мережу від єдиної точки відмови, наприклад, відімкнення мережного кабелю або несправності комутатора. Проте, при запровадженні фізичної надлишковості у мережі, можуть виникати зациклювання та дублювання кадрів, Протокол єднального дерева (Spanning Tree Protocol, STP) допомагає розв'язати ці проблеми. Основна функція STP полягає у запобіганні появі петель у мережі на основі комутаторів.

Засоби адміністративного контролю доступу

Засоби адміністративного контролю доступу - це політики та процедури, визначені організацією для впровадження і забезпечення дотримання всіх аспектів контролю несанкціонованого доступу.



- Політики - це твердження про наміри.
- Процедури - це докладні кроки, необхідні для виконання певних дій.
- Практика найму співробітників передбачає кроки, яких вживає організація для пошуку кваліфікованих співробітників.
- Перевірка біографії - це тип перевірки інформації про співробітників, яка стосується даних з попередніх місць працевлаштування, кредитної історії та наявності судимостей.
- Класифікація даних впорядковує їх по категоріях на основі рівня секретності.
- Тренінги з питань безпеки інформують співробітників про політики безпеки, які діють в організації.
- Ревізії оцінюють ефективність роботи співробітника.

Що таке ідентифікація?

Ідентифікація забезпечує дотримання правил, встановлених політикою авторизації. Щоразу при зверненні до певного ресурсу, елементи контролю доступу вирішують, надати або заборонити доступ.

Унікальний ідентифікатор забезпечує належний зв'язок між дозволеними діями та суб'єктами. Найчастіше користувача ідентифікують за його іменем.

Унікальний ідентифікатор гарантує, що система зможе вирізнити кожну конкретну особу, що дасть змогу авторизованому користувачеві виконувати необхідні дії на конкретному ресурсі.

Безпека нульової довіри

Нульова довіра (Zero trust) – це комплексний підхід до всебічного захисту доступу в мережах, програмах і середовищах. Він допомагає забезпечити надійний доступ з боку користувачів, їх кінцевих пристроїв, API, Інтернету речей, мікросервісів, контейнерів тощо, чим захищає співробітників організації, їх робоче навантаження та робоче місце.

Нульова довіра до робочої сили
: Цей компонент стосується, які мають доступ до робочих програм зі своїх персональних або корпоративних пристроїв. Ця система гарантує, що лише визначені користувачі та захищені пристрої можуть звертатися до програм, незалежно від місця розташування.

Нульова довіра до робочих навантажень
: Цей рівень стосується програм, які працюють у хмарі, центрах обробки даних та інших віртуалізованих середовищах, які взаємодіють одне з одним. Він має на меті убезпечити доступ API, мікросервісів або контейнерів до бази даних у межах застосунку.

Нульова довіра до робочого місця
: Цей рівень зосереджений на наданні безпечного доступу будь-якому компоненту корпоративних мереж, як-от пристроям Інтернету речей (IoT), кінцевим вузлам користувачів, фізичним і віртуальним серверам, принтерам, камерам, системам HVAC, інфузійним насосам, системам керування виробництвом та багатьом іншим.

Моделі контролю доступу

- Вибірковий контроль доступу - це модель із найменшими обмеженнями, яка дає змогу користувачам, як власникам даних, контролювати доступ до них. DAC може використовувати ACL або інші методи для визначення того, які користувачі або групи користувачів мають доступ до інформації.
- Обов'язковий контроль доступу - запроваджує жорсткіший контроль доступу і зазвичай використовується у військових цілях або у критично важливих системах. Для різних типів інформації застосовується маркування безпеки, а користувачі одержують доступ на основі визначеного рівня захисту.
- Контроль доступу на основі ролей - рішення щодо доступу базуються на ролях та рівнях відповідальності осіб всередині організації. Кожна роль передбачає призначення відповідних привілеїв безпеки та створення профілю RBAC, до яких згодом долучають користувачів.
- Контроль доступу на основі правил - співробітники служби безпеки мережі визначають набори правил щодо умов, які пов'язані з доступом до даних або систем.