Лекція 25. Захист Web застосунків

https://www.javatpoint.com/cyber-security-tutorial

Кібербезпека - це захист інтернет-зв'язаних систем, включаючи апаратне забезпечення, програмне забезпечення та дані від кібератак. Вона передбачає взаємодію людей, процесів та технологій для охоплення повного спектру зменшення загроз, зниження вразливості, запобігання інформаційних ризиків, міжнародної співпраці та політики відновлення та діяльності, включаючи операції комп'ютерних мереж, забезпечення інформаційної безпеки, правоохоронну діяльність тощо.

Під кібербезпекою розуміють сукупність технологій, процесів та практик, спрямованих на захист мереж, пристроїв, програм та даних від атак, крадіжок, пошкоджень, модифікацій або несанкціонованого доступу. Тому його також можна називати безпекою інформаційних технологій.

Кібератаки наразі є міжнародною проблемою, яка викликає багато занепокоєнь, що можуть загрожувати глобальній економіці. Зі зростанням обсягу кібератак, компанії та організації, особливо ті, що працюють з інформацією, пов'язаною з національною безпекою, здоров'ям або фінансовими записами, повинні приймати заходи для захисту своєї чутливої бізнесової та особистої інформації.

25.1 Поняття «кібербезпека»

Техніка захисту систем, підключених до Інтернету, таких як комп'ютери, сервери, мобільні пристрої, електронні системи, мережі та дані від зловмисних атак, називається кібербезпекою. Термін «кібербезпека» можена розділити на дві частини: «кібер» та «безпека». Перша частина відноситься до технології, що включає системи, мережі, програми та дані. А друга стосується захисту систем, мереж, додатків та інформації. У деяких випадках її також називають електронною інформаційною безпекою або безпекою інформаційних технологій.

Інші визначення кібербезпеки:

"Кібербезпека – це сукупність технологій, процесів та практик, спрямованих на захист мереж, пристроїв, програм та даних від атак, крадіжок, пошкоджень, модифікацій або несанкціонованого доступу."

"Кібербезпека – це набір принципів та практик, спрямованих на захист наших обчислювальних ресурсів та онлайн-інформації від загроз."

25.2 Типи кібербезпеки

Активи кожної організації є комбінацією різних систем. Ці системи мають міцну кібербезпеку, що вимагає спільних зусиль у всіх її системах. Тому, можна розбити кібербезпеку на наступні категорії:

1 **Мережева безпека**: включає в себе використання апаратного та програмного забезпечення для захисту комп'ютерної мережі від несанкціонованого доступу, вторгнень, атак, збоїв та зловживань. Ця безпека допомагає організації захищати свої активи від зовнішніх та внутрішніх загроз.

2 **Безпека додатків**: включає захист програмного забезпечення та пристроїв від небажаних загроз. Цей захист може бути забезпечений постійним оновленням застосунків для забезпечення їх захисту від атак. Успішна безпека починається на етапі проєктування, написання вихідного коду, перевірки, моделювання загроз тощо, перед випуском програми або пристрою в експлуатацію.

3 **Інформаційна або даних безпека**: включає в себе використання надійних механізмів зберігання даних для забезпечення цілісності та конфіденційності даних як піл час зберігання, так і в процесі передачі.

4 **Управління ідентифікацією**: полягає у реалізації процедурии визначення рівня доступу кожної особи в організації до різних інформаційних ресурсів.

5 **Операційна безпека**: включає обробку та прийняття рішень щодо обробки та захисту інформаційних ресурсів.

6 **Інформаційна безпека у хмарі**: включає в себе захист інформації, яка зберігається в цифровому середовищі або хмарних архітектурах для організації. Використовуються різні постачальники хмарних послуг, такі як AWS, Azure, Google тощо, щоб забезпечити безпеку проти різних загроз.

7 **Відновлення після катастрофи та планування неперервності бізнесу**: реалізує моніторинг, оповіщення та планування заходів реагування на втрату операцій або даних внаслідок будь-якої зловмисної діяльності. Політика реагування визначає відновлення втрачених операцій після будь-якої катастрофи до такої ж міри функціонування, як і до події.

8 **Освіта користувачів**: займається проведенням тренінгів та інших заходів з підвищення навичок та свідомості в сфері захисту інформаційних ресурсів.

25.3 Важливість та цілі кібербезпеки

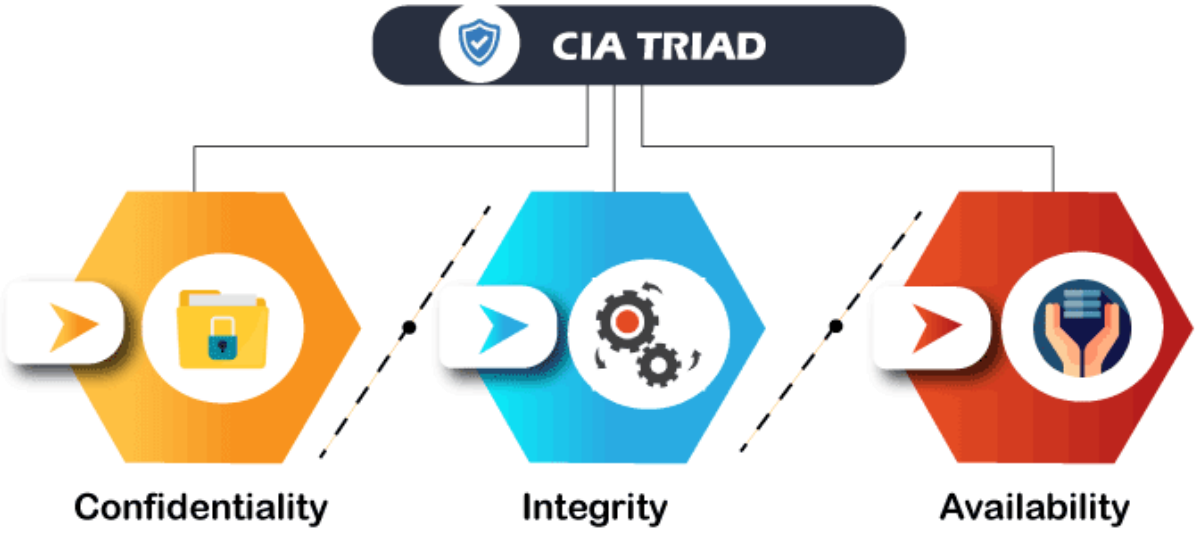
Сьогодні ми живемо в цифрову еру, де всі аспекти нашого життя залежать від мереж, комп'ютерів та інших електронних пристроїв та програмних додатків. Всі критичні інфраструктури, такі як банківська система, охорона здоров'я, фінансові установи, уряди та виробничі галузі, використовують пристрої, підключені до Інтернету, як основну складову своєї діяльності. Деяка інформація, така як інтелектуальна власність, фінансові дані та особисті дані, може бути чутливою для несанкціонованого доступу або розголошення, що може мати негативні наслідки. Ця інформація дає зловмисникам та загрозам можливість проникнення для отримання фінансової вигоди, вимагання викупу, політичних або соціальних мотивів або просто вандалізму.

Кібератаки тепер стали міжнародною проблемою, яка може зламувати систему та інші атаки на безпеку можуть загрожувати світовій економіці. Тому важливо мати відмінну стратегію кібербезпеки для захисту чутливої інформації від високопрофільних порушень безпеки. Крім того, зі зростанням обсягу кібератак компанії та організації, особливо ті, що працюють з інформацією, пов'язаною з національною безпекою, охороною здоров'я або фінансовими документами, повинні використовувати потужні заходи кібербезпеки та надійні процеси для захисту своєї чутливої бізнесової та особистої інформації.

Основною метою кібербезпеки є забезпечення захисту даних. Спільнота забезпечення безпеки надає три пов'язані принципи для захисту даних від кібератак. Цей принцип називається триадою CIA.

Модель CIA призначена для управління політикою інформаційної безпеки організації. Коли виявляються будь-які порушення безпеки, це означає, що один або декілька з цих принципів були порушені.

Можна розбити модель CIA на три частини: конфіденційність, цілісність та надійність. Така модель безпеки допомагає структурувати процес захисту інформаційних ресурсів на окремі частини IT-безпеки. Розглянемо кожну частину детальніше.



Конфіденційність є еквівалентом приватності, яка запобігає несанкціонованому доступу до інформації. Вона передбачає забезпечення доступності даних для індивідів, які мають право на їх використання, та блокування доступу для всіх інших. Це перешкоджає потраплянню важливої інформації до неправильних людей. Іншим ефективним методом забезпечення конфіденційності є шифрування даних.

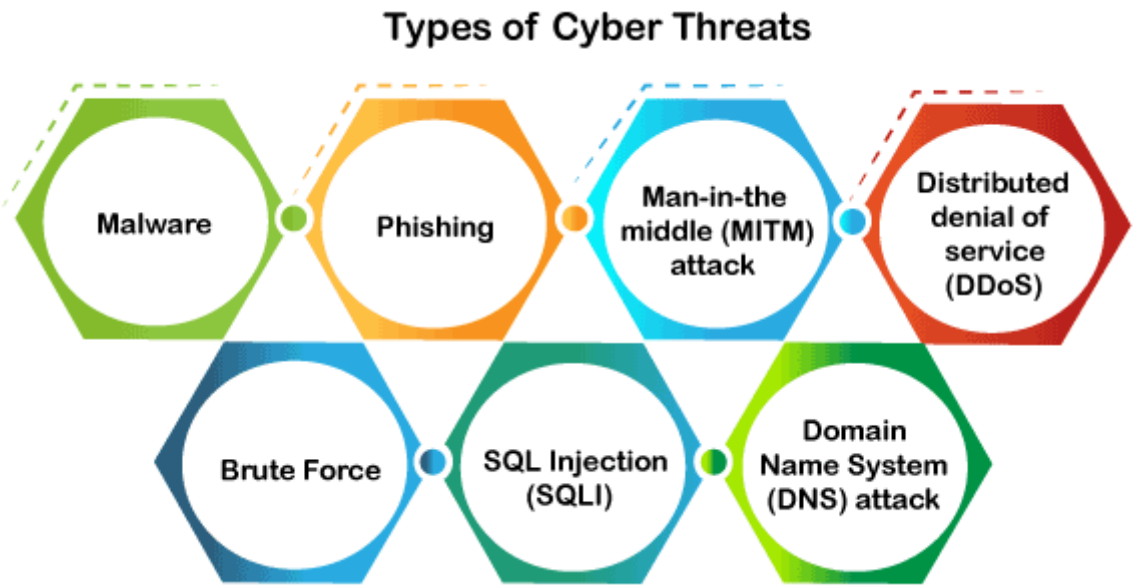
Цілісність – це принцип, який забезпечує аутентичність даних, їх точність та захищеність від несанкціонованої модифікації з боку зловмисників або несвідомих користувачів. Якщо відбувається будь-яка модифікація, необхідно вжити певних заходів для захисту чутливих даних від пошкодження або втрати та швидко відновити систему після такої події.

Надійність – це принцип, який забезпечує доступність інформації та її корисність для авторизованих осіб завжди. Він забезпечує, що ці

доступи не будуть перешкоджені внаслідок несправності системи або кібератак.

25.4 Типи загроз кібербезпеці

Загроза в кібербезпеці – це зловживання фізичною або юридичною особою з метою порушення або крадіжки даних, отримання доступу до мережі або заваджання цифровому життю взагалі. Кіберспільнота визначає наступні загрози, що існують сьогодні:



25.4.1 Шкідливе програмне забезпечення (Malware)

Шкідливе програмне забезпечення означає зловмисне програмне забезпечення, яке є найпоширенішим інструментом кібератак. Воно використовується кіберзлочинцем або хакером, щоб завадити або пошкодити систему законного користувача. Існують такі важливі типи шкідливого програмного забезпечення:

1) вірус – це зловмисний код, який поширюється з одного пристрою на інший, може очищати файли та поширюватися по всій системі комп'ютера, інфікуючи файли, крадучи інформацію або завдаючи шкоди пристроєві;

2) шпигунське програмне забезпечення (Spyware) – це програмне забезпечення, яке таємно записує інформацію про дії користувача на їхній системі, наприклад, шпигунське програмне забезпечення може захоплювати дані кредитної картки, які можуть бути використані кіберзлочинцями для несанкціонованих покупок, зняття грошей тощо;

3) троян (Trojans) – це тип шкідливого програмного забезпечення або коду, який з'являється як законне програмне забезпечення або файл, щоб обдурити систему піл час у завантаження та запуску, його основною метою є порушення або крадіжка даних з нашого пристрою або виконання інших шкідливих дій в нашій мережі;

4) здирницьке програмне забезпечення (Ransomware) – це програмне забезпечення, яке шифрує файли та дані користувача на пристрої, зробивши їх непридатними для використання або видаляючи їх, потім зловмисники вимагають викуп у грошовій формі для дешифрування.

5) хробаки (Worms) – Це програмне забезпечення, яке поширює копії самого себе з пристрою на пристрій без участі людини, хробакам не потрібно приєднуватися до будь-якої програми, щоб викрасти або пошкодити дані;

6) рекламне програмне забезпечення (Adware) – це рекламне програмне забезпечення, яке використовується для поширення шкідливих програм та відображення реклами на нашому пристрої, це небажана програма, яка встановлюється без дозволу користувача, основною метою якої є генерація прибутку для її розробника, показуючи реклами у браузері;

7) ботмережі (Botnets) – це збірка підключених до Інтернету пристроїв, які заражені шкідливим програмним забезпеченням, що дозволяє кіберзлочинцям керувати ними. Це дозволяє кіберзлочинцям отримувати витоки облікових даних, несанкціонований доступ та крадіжку даних без дозволу користувача.

25.4.2 Фішинг (Phishing)

Фішинг – це тип кіберзлочинності, при якому відправник здається справжньою організацією, такою як PayPal, eBay, фінансовою установою, другом або колегою. Він зв'язується з цільовим або кількома цільовими особами за допомогою електронної пошти, телефону або текстового повідомлення з посиланням, щоб переконати їх натиснути на це посилання. Це посилання перенаправить їх на шахрайські веб-сайти, де їм буде запропоновано надати конфіденційні дані, такі як особиста

інформація, банківська і кредитна інформація, номера соціального забезпечення, імена користувачів та паролі. Натискання на посилання також дозволить встановлювати шкідливе програмне забезпечення на пристроях цільових осіб, що дозволяє хакерам дистанційно керувати пристроями.

25.4.3 Атака "людина посередині" (Man-in-the-middle attack або MITM)

Атака "людина посередині" – це тип кіберзагрози (форма атаки прослуховування), при якому кіберзлочинець перехоплює розмову або передачу даних між двома особами. Щойно кіберзлочинець опиняється посередині комунікації двох сторін, він здається справжнім учасником і може отримувати конфіденційну інформацію та надсилати різні відповіді. Основною метою цього типу атак є отримання доступу до наших бізнесових або клієнтських даних. Наприклад, кіберзлочинець може перехоплювати дані, що передаються між цільовим пристроєм та мережею на незахищеній Wi-Fi мережі.

25.4.4 Розподілена атака на забезпечення послуг (DDoS)

Це тип кіберзагрози або зловмисної спроби, коли кіберзлочинці переривають нормальний трафік на цілі сервери, послуги або мережі, виконуючи законні запити до цільової або суміжної інфраструктури з Інтернет-трафіку. Тут запити надходять з кількох IP-адрес, що може зробити систему непридатною до використання, перевантажити сервери, значно уповільнити їх або тимчасово призупинити їх роботу, або перешкодити організації здійснювати свої важливі функції.

25.4.5 Атака методом перебору (Brute Force)

Атака методом перебору – це криптографічний хак, який використовує метод спроб і помилок для вгадування всіх можливих комбінацій, поки не буде виявлена правильна інформація. Кіберзлочинці зазвичай використовують цю атаку для отримання особистої інформації про цільові паролі, дані входу, ключі шифрування та персональні ідентифікаційні номери (PIN).

25.4.6 SQL-ін'єкція (SQLI)

SQL-ін'єкція є поширеною атакою, яка відбувається, коли кіберзлочинці використовують шкідливі SQL-скрипти для

маніпулювання базами даних з метою доступу до конфіденційної інформації. Після успішної атаки зловмисник може переглядати, змінювати або видаляти конфіденційні корпоративні дані, списки користувачів або приватні деталі клієнтів, які зберігаються в базі даних SQL.

25.4.7 Атака на систему доменних імен (DNS)

Атака на систему доменних імен (DNS) – це тип кібератаки, при якій кіберзлочинці використовують недоліки в системі доменних імен, щоб перенаправляти користувачів сайту на зловмисні веб-сайти (хищення DNS) та викрадати дані з пошкоджених комп'ютерів. Це серйозний кібербезпечний ризик, оскільки система DNS є важливим елементом інфраструктури Інтернету.

Наступні кіберзагрози були виявлені урядами Великої Британії, США та Австралії.

25.4.8 Романтичні шахрайства

Цю кіберзагрозу уряд США виявив у лютому 2020 року. Кіберзлочинці використовують цю загрозу через сайти знайомств, чати та застосунки. Вони атакують людей, які шукають нового партнера, і змушують їх надавати особисті дані.

25.4.9 Вірус Dridex

Це тип фінансового троянського вірусу, який був ідентифікований урядом США у грудні 2019 року і впливає на громадськість, урядові структури, інфраструктуру та бізнес по всьому світу. Він заражає комп'ютери через фішингові електронні листи або існуюче шкідливе програмне забезпечення, щоб викрасти конфіденційну інформацію, таку як паролі, банківські реквізити та особисті дані для шахрайських транзакцій. Національний центр кібербезпеки Великої Британії закликає людей переконатися, що їхні пристрої мають установлені оновлення, включений та оновлений антивірус, а також наявність резервних копій файлів для захисту конфіденційних даних від цієї атаки.

25.4.10 Вірус Emotet

Emotet є типом кібератаки, який викрадає конфіденційну інформацію та також встановлює інші шкідливі програми на вашому

пристрої. Від цієї глобальної кіберзагрози національні організації були попереджені Австралійським центром кібербезпеки в 2019 році.

Наступні системи можуть підлягати порушенням безпеки та кібератакам:

Комунікації: кіберзлочинці можуть використовувати телефонні дзвінки, електронні листи, текстові повідомлення та додатки для обміну повідомленнями для кібератак.

Фінанси: ця система має справу з ризиком фінансової інформації, такої як банківські та кредитні картки, така інформація зазвичай є основною метою кіберзлочинців.

Урядові структури: кіберзлочинці, як правило, спрямовують свої атаки на установи уряду, щоб отримати конфіденційні публічні дані або приватну інформацію громадян.

Транспорт: у цій системі кіберзлочинці, як правило, спрямовують свої атаки на підключені автомобілі, системи керування трафіком та інфраструктуру розумних доріг.

Охорона здоров'я: кіберзлочинці спрямовують свої атаки на систему охорони здоров'я, щоб отримати інформацію, яка зберігається в місцевій клініці або критичних системах догляду в національних лікарнях.

Освіта: кіберзлочинці спрямовують свої атаки на освітні установи, щоб отримати конфіденційні дослідження та інформацію про студентів та працівників.

Переваги кібербезпеки:

1 Захист від кібератак та порушень даних для бізнесу.

2 Захист даних та мережі.

3 Уникнення несанкціонованого доступу користувачів.

4 Швидший час відновлення після порушення безпеки.

5 Захист кінцевих користувачів та кінцевих пристроїв.

6 Відповідність регуляторним вимогам.

7 Континуїтет операцій.

8 Збереження репутації компанії та довіри з боку розробників, партнерів, споживачів, зацікавлених сторони та працівників.

25.5 Загальні поради з кібербезпеки:

Проведення тренінгів з кібербезпеки та збільшення обізнаності. Кожна організація повинна навчати свій персонал кібербезпеці, політикам компанії та повідомленням про інциденти, щоб успішно реалізувати політику кібербезпеки. Якщо працівники вчиняють ненавмисні або навмисні зловживання, це може призвести до порушення технічних захистів, результатом якого є порушення безпеки та значні втрати в основній діяльності компанії. Тому варто проводити тренінги та навчання для персоналу через семінари, курси та онлайн-курси, що зменшує кількість порушень безпеки.

Оновлення програмного забезпечення та операційнх систем. Найпопулярнішим заходом безпеки є оновлення програмного забезпечення та ОС для отримання переваг останніх заходів безпеки.

Використання антивірусного програмного забезпеченняж. Слід використовувати антивірусне програмне забезпечення, яке виявляє та видаляє небажані загрози з вашого пристрою. Це програмне забезпечення завжди оновлюється, щоб забезпечити найвищий рівень захисту.

Виконання періодичних перевірок безпеки. Кожна організація здійснює періодичні перевірки безпеки всього програмного забезпечення та мереж для виявлення ризиків безпеки на ранніх етапах в безпечному середовищі. Деякі популярні приклади перевірок безпеки – це тестування проникнення додатків та мереж, огляд джерел коду, огляд архітектури дизайну та оцінювання ризиків. Крім того, організації повинні пріоритезувати та якнайшвидше ліквідовувати виявлені уразливості безпеки.

Використання складних паролів. Рекомендується використовувати довгі паролі, які складаються з різних комбінацій символів та знаків. Це робить паролі менш передбачуваними.

Ігнорування електронних листів від невідомих відправників. Кіберексперти завжди радять не відкривати або не клікати по електронних листах, що надходять від неперевірених відправників або з незнайомих веб-сайтів, оскільки вони можуть містити шкідливе програмне забезпечення.

Уникання використання незахищених Wi-Fi мереж у громадських місцях. Експерти також радять уникати використання ненадійних мереж, оскільки вони можуть залишити вас вразливими до атак "людина посередині".

Резервне копіювання даних. Кожна організація повинна періодично робити резервне копіювання своїх даних, щоб забезпечити, що всі чутливі дані не будуть втрачені або відновлені після порушення безпеки. Крім того, резервні копії можуть допомогти зберегти цілісність даних під час кібератак, таких як SQL-ін'єкції, фішинг та розшифрування даних.

25.6 Історія кібербезпеки.

Початок кібербезпеки пов'язаний з досліджувальним проектом, запущеним у 1970-х роках. Цей проект мав назву ARPANET (Advanced Research Projects Agency Network), був мережею комп'ютерів, створеною для обміну даними та спілкування між науковцями. Однак зі зростанням мережі зросла й загроза кібератак. Перший комп'ютерний вірус був створений у 1971 році, що призвело до створення першого антивірусного програмного забезпечення в 1980-х. Сьогодні кібербезпека є важливою складовою будь-яких операцій організації, а галузь постійно розвивається, щоб бути в курсі нових загроз та вразливостей.

У 1969 році Леонард Кляйнрок, професор UCLA, та студент Чарлі Клайн відправили перше електронне повідомлення з комп'ютера UCLA SDS Sigma 7 до програміста Біла Дювала в Stanford Research Institute. Ця історія стала добре відомою та моментом в історії цифрового світу. Відправлене повідомлення з UCLA містило слово "login". Система впала

після того, як вони набрали перші дві літери "lo". З того часу ця історія стала переконанням, що програмісти набрали початкове повідомлення "lo and behold". Фактично ж було призначене повідомлення "login". Ці дві літери повідомлення змінили спосіб, яким ми спілкуємося один з одним.

У 1970-х роках Роберт (Боб) Томас, дослідник компанії BBN Technologies з Кембриджа, штат Массачусетс, створив перший комп'ютерний хробак (вірус). Він зрозумів, що комп'ютерна програма може переміщуватись по мережі, залишаючи за собою маленький слід (послідовність знаків). Він назвав програму Creeper і розробив її для переміщення між терміналами Tenex на ранній версії ARPANET, завдяки повідомленню "I'M THE CREEPER: CATCH ME IF YOU CAN".

Рей Томлінсон, американський програміст, винахідник електронної пошти, також тоді працював у BBN Technologies. Він вподобав цю ідею та трохи попрацював з програмою, зробив її самореплікуючоюся тобто "першим комп'ютерним хробаком". Він назвав програму Reaper, першим антивірусним програмним забезпеченням, яке знаходило копії Creeper і видаляло їх.

Після Creeper і Reaper кіберзлочини стали більш потужними. З розвитком комп'ютерного програмного та апаратного забезпечення злами безпеки також зросли. У 1986 році Росія стала першою країною, яка використовувала кіберзброю як зброю. Німецький громадянин Маркус Гесс взломав 400 військових комп'ютерів, включаючи процесори у Пентагоні. Він планував продати таємниці КГБ, але американський астроном Кліффорд Столл зловив його до того, як це сталося.

У 1988 році американський комп'ютерний вчений Роберт Морріс хотів перевірити розмір Інтернету. Він написав програму для тестування розміру Інтернету. Ця програма проходила через мережі, вторгалася в Unix термінали та копіювалася. Програма стала першим відомим мережевим вірусом і отримала назву Моріс-хробак або Інтернет-хробак.

Моріс-хробак міг інфікувати комп'ютер кілька разів, а кожен додатковий процес сповільнював роботу машини, що в кінцевому результаті призводило до її пошкодження. Роберт Морріс був звинувачений за Законом про комп'ютерні злочини та зловживання. Сам закон призвів до створення Команди реагування на комп'ютерні екстрені ситуації. Це некомерційний дослідницький центр для проблем, які можуть загрожувати Інтернету в цілому.

В даний час віруси стали більш смертоносними, більш інвазивними та важкими для контролю. Вищезазначене – це лише деякі приклади, але цих атак достатньо, щоб довести, що кібербезпека є необхідністю як для корпорацій, так і для малих бізнесів.

Ціль кібербезпеки полягає у захисті інформації від крадіжок, компрометацій або атак. Кібербезпеку можна виміряти за допомогою однієї з трьох цілей:

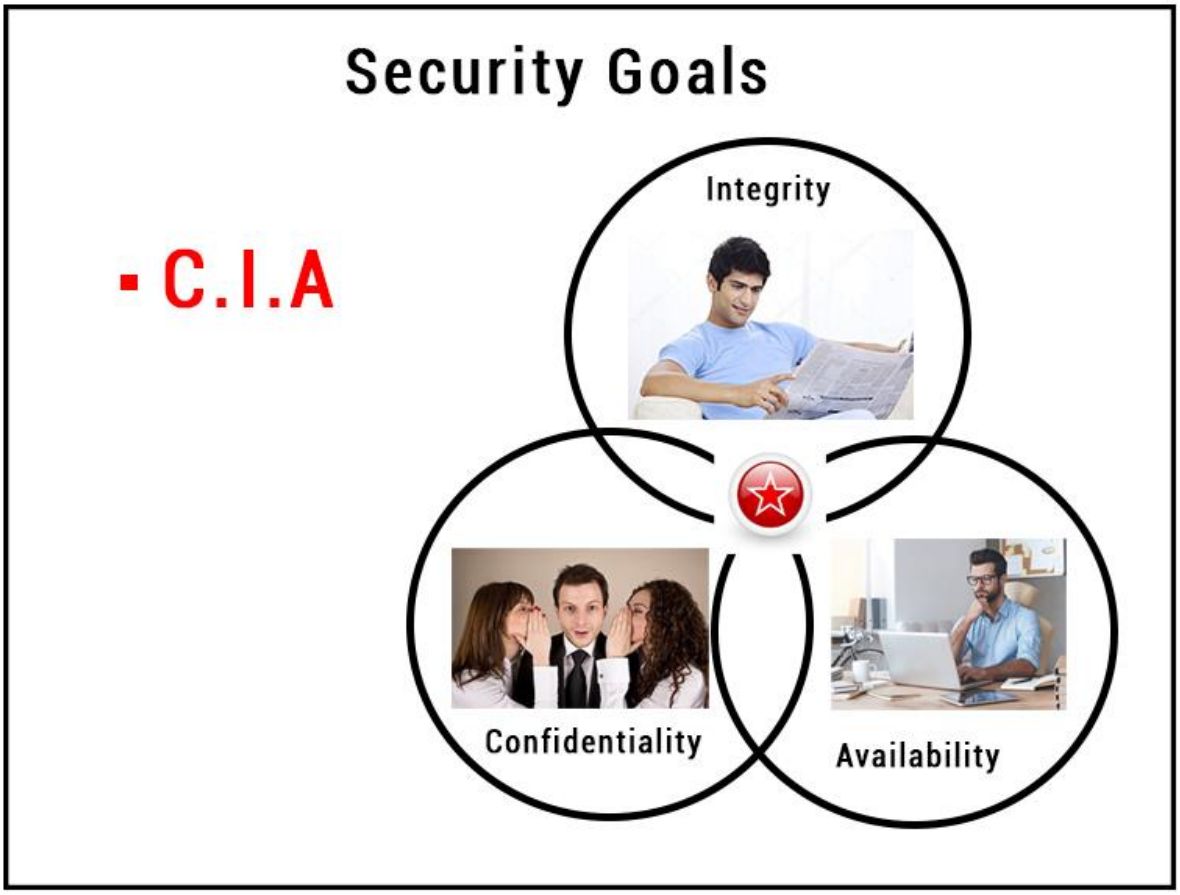
Захист конфіденційності даних.

Збереження цілісності даних.

Забезпечення доступності даних для авторизованих користувачів.

Ці цілі утворюють триаду конфіденційності, цілісності та доступності (CIA), основу всіх програм забезпечення безпеки. Триада CIA є моделлю безпеки, яка призначена для керування політиками з інформаційної безпеки в межах організації або компанії. Цю модель також називають триадою AIC (доступність, цілісність та конфіденційність)

Критерії CIA використовують більшість організацій і компаній, коли вони встановлюють нову програму, створюють базу даних або гарантують доступ до деяких даних. Для повної безпеки даних всі ці цілі безпеки повинні бути виконані. Це політики безпеки, які всі працюють разом.



1 Конфіденційність

Конфіденційність запобігає потраплянню важливої інформації до осіб, які не мають на неї прав, та одночасно забезпечує отримання цієї інформації особами, які мають права на її отримання.

Деякі засоби для забезпечення конфіденційності включають:

1 Програмне забезпечення шифрування: використовується для кодування даних та запобігання несанкціонованого доступу.

2 Контроль доступу: обмежує доступ до даних, дозволяючи доступ до інформації лише авторизованим користувачам.

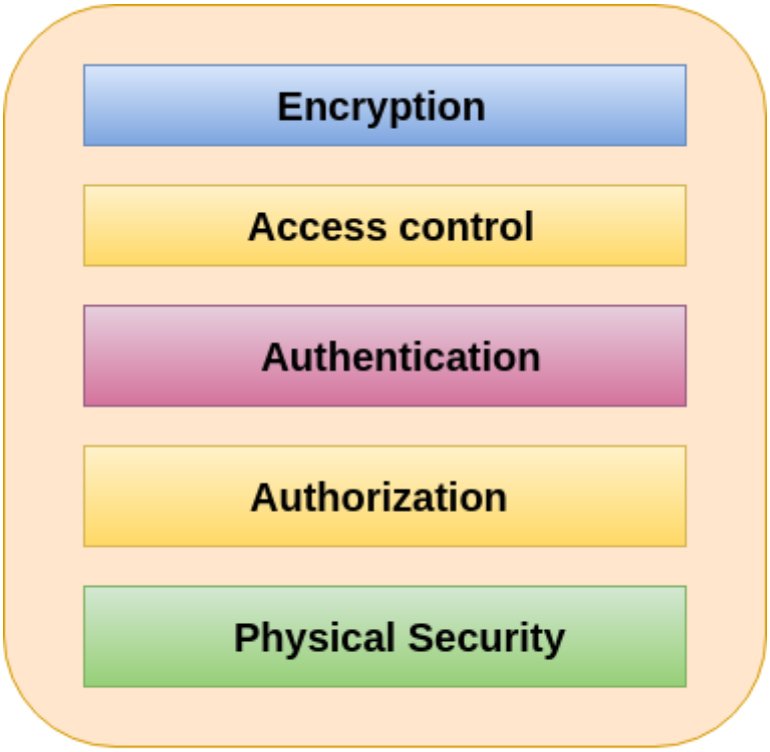
3 Брандмауери: діє як бар'єр, щоб запобігти несанкціонованому доступу до мережі.

4 Віртуальні приватні мережі (VPN): шифрує інтернет-трафік для захисту онлайн-комунікацій.

5 Запобігання втраті даних (DLP): відслідковує та контролює конфіденційні дані, щоб запобігти їх витоку з мережі організації.

6 Політики паролів: забезпечує, що користувачі створюють надійні паролі та періодично змінюють їх, щоб запобігти несанкціонованому доступу до своїх облікових записів.

7 Багатофакторна аутентифікація (MFA): додає додатковий рівень безпеки, вимагаючи більше одного способу аутентифікації, такого як пароль та сканування відбитка пальця, для доступу до даних.



Confidentiality Tools

Шифрування є методом перетворення інформації з метою зробити її незрозумілою для несанкціонованих користувачів, використовуючи алгоритм. Трансформація даних використовує секретний ключ (ключ шифрування), щоб перетворені дані можна було прочитати лише за допомогою іншого секретного ключа (ключа дешифрування). Це захищає чутливі дані, такі як номери кредитних карток, шифруючи та перетворюючи дані на незрозумілий для розуміння текст-шифр. Ці зашифровані дані можна прочитати лише розшифрувавши їх. Асиметричне та симетричне шифрування є двома основними типами шифрування.

Контроль доступу визначає правила та політики, які обмежують доступ до системи або фізичних та віртуальних ресурсів. Це процес, за яким користувачам надаються доступ та певні привілеї до систем, ресурсів або інформації. У системах контролю доступу користувачі повинні надати облікові дані перед отриманням доступу, такі як ім'я людини або серійний номер комп'ютера. У фізичних системах такі облікові дані можуть мати багато форм, але найбільш безпечними є облікові дані, які не можна передавати.

Аутентифікація – це процес, що забезпечує підтвердження і підтверджує ідентифікацію користувача або ролі, яку він виконує. Це може бути зроблено за допомогою різних методів, але зазвичай воно ґрунтується на комбінації наступних даних:

– дані про пристрій користувача (наприклад, смарт-карту або радіоключ для зберігання секретних ключів),

– дані, які користувач знає (наприклад, пароль),

– біометричні дані користувача (наприклад, відбиток пальця).

Аутентифікація є необхідністю для кожної організації, оскільки вона дозволяє організаціям зберігати безпеку їх мереж, дозволяючи доступ лише аутентифікованим користувачам до захищених ресурсів. Ці ресурси можуть включати комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві застосунки або служби.

Авторизація є механізмом безпеки, який надає дозвіл на виконання або отримання даних. Вона використовується для визначення того, чи дозволено конкретній особі або системі отримати доступ до ресурсів, таких як комп'ютерні програми, файли, сервіси, дані та можливості додатків. Зазвичай перед авторизацією проводиться перевірка ідентифікації користувача. Адміністратори систем зазвичай мають рівні дозволів, що охоплюють всі ресурси системи та користувачів. Під час авторизації система перевіряє правила доступу аутентифікованого користувача та надає або відмовляє у доступі до ресурсів.

Фізична безпека описує заходи, спрямовані на запобігання несанкціонованому доступу до IT-активів, таких як приміщення, обладнання, персонал, ресурси та інші майнові цінності від

пошкодження. Вона захищає ці активи від фізичних загроз, таких як крадіжка, вандалізм, пожежа та природні катастрофи.

2 Цілісність

Цілісність забезпечює адекватність, точність та захищеність від несанкціонованої модифікації користувачами.

Існує кілька способів забезпечення цілісності даних, включаючи наступні:

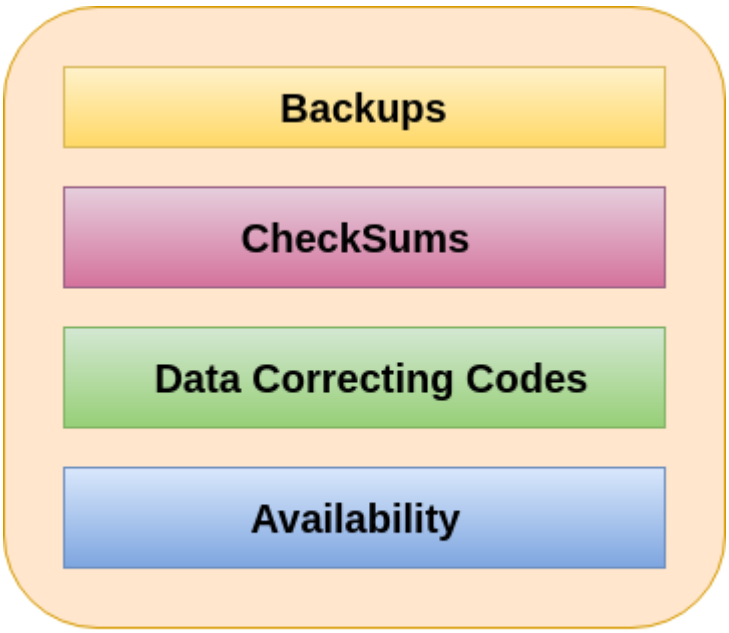
1. Хеш-функції: використовуються для генерації фіксованої довжини блоку даних, що репрезентує оригінальні дані. Цей блок можна перевірити на наявність змін, порівнюючи новий блок зі старим блоком.

2. Цифрові підписи: використовуються для підтвердження автентичності інформації та забезпечення її незмінності. Цифровий підпис забезпечує захист від підробки, забезпечуючи те, що лише автор підписав документ.

3. Резервне копіювання даних: забезпечує збереження даних від збоїв апаратного забезпечення або програмного забезпечення. Резервна копія забезпечує збереження оригінальних даних, які можуть бути відновлені, якщо оригінал втрачено або пошкоджено.

4. Аудит: використовується для відстеження змін в системі або базі даних. Журнали аудиту містять записи про всі дії користувачів, які взаємодіють з даними, та дозволяють виявити будь-які недоречності або зловживання.

Ці інструменти допомагають забезпечити цілісність даних та зменшити ризик їх порушення.



Integrity Tools

Резервне копіювання є періодичним архівуванням даних. Це процес створення копій даних або файлів з метою використання у випадку втрати або знищення оригінальних даних або файлів. Також використовується для створення копій для історичних цілей, таких як довготривалі дослідження, статистика або для збереження історичних даних або відповідно до політики зберігання даних. Багато програм, особливо в середовищі Windows, створюють файли резервних копій з розширенням файлу .BAK.

Контрольна сума – це числове значення, що використовується для перевірки цілісності файлу або передачі даних. Іншими словами, це обчислення функції, яка відображає вміст файлу на числове значення. Вони, як правило, використовуються для порівняння двох наборів даних, щоб переконатися, що вони співпадають. Функція контрольної суми залежить від усього вмісту файлу. Вона розроблена таким чином, що навіть невелика зміна вхідного файлу (наприклад, перестановка одного біту) імовірно приведе до різних значень вихідних даних.

Коди корекції даних – це метод зберігання даних таким чином, що невеликі зміни можуть бути легко виявлені та автоматично виправлені.

3 Доступність

Доступність – це властивість, за якої інформація є доступною та може бути змінена вчасно тими, хто має на це право. Це гарантія

надійного та постійного доступу до наших конфіденційних даних для авторизованих осіб.

Інструменти для забезпечення доступності: фізичні заходи захисту, обчислювальні резервування

Фізичний захист означає збереження інформації доступною навіть у разі фізичних проблем. Він забезпечує збереження конфіденційної і критичної інформації в безпечних місцях.

Обчислювальні резервування застосовується як безвідмовність при випадкових помилках. Він захищає комп'ютери та пристрої зберігання, які служать як запасні в разі відмов.

Деякі інструменти забезпечення доступності даних включають:

1 Резервне копіювання: Це процес створення копій даних або файлів даних для використання в разі втрати або знищення оригінальних даних або файлів даних.

2 Кластеризація: Це процес збільшення доступності даних за рахунок розподілу даних на кілька серверів.

3 Резервне електроживлення: Це система, яка забезпечує постійну електропостачання для комп'ютерів і серверів, навіть у випадку перебоїв в роботі електромережі.

4 Керованість завантаженням: Це інструмент, який розподіляє навантаження на сервери, щоб збільшити доступність даних.

5 Відмовостійкість: Це забезпечення доступності даних в разі відмови одного або кількох компонентів системи.

6 Моніторинг мережі: Це інструмент, який дозволяє вести моніторинг доступності даних в реальному часі та оперативно виявляти проблеми.