Захист персональних даних в темедичних та медичних інформаційних системах

З метою організації медичного захисту інформації України, телемедична система є інформаційною системою, що обробляє спеціальні категорії персональних даних, що стосуються стану здоров'я суб'єктів персональних даних і вимагає **не нижче 3-го рівня захищеності** персональних даних.

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

У тому ж законі про інформацію поняття захист інформації визначається як, сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Захист – засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні, в тому числі програмні, заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

Метод захисту (protection method) – система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним або апаратним способом.

Захист інформації ведеться з метою підтримки таких властивостей інформації як:

- цілісність – неможливість модифікації інформації неавторизованим користувачем. Цілісність інформації важливий аспект інформаційної безпеки, що забезпечує запобігання несанкціонованих змін та руйнування інформації.

Цілісність, це стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи;

автоматичне відновлення у випадку виявлення системою потенційної помилки;

автоматичне використання альтернтивних компонентів замість тих, що вийшли зладу;

- конфіденційність – інформація не може бути отримана неавторизованим користувачем. Треба захисти інформацію від несанкціонованого ознайомлення з нею.

- доступність – полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

В інформаційній системі медичного закладу об’єктами захисту є:

– інформація в базах даних (БД) систем керування базами даних (СКБД);

– ресурси файлового сервера лікувально-профілактичного закладу;

– резервні копії БД СКБД і архівні копії ресурсів файлового сервера;

– керуюча інформація операційної системи, СКБД, автоматизоване робоче місце (АРМ) адміністратора медичної інформаційної системи (МІС) та інженера інформаційної безпеки (ІБ);

– технологічний процес збору, обробки, зберігання та передачі інформації в МІС;

– апаратно-програмний комплекс, що забезпечує роботу МІС.

Інформаційна безпека забезпечується спеціальними програмними засобами – підсистемою інформаційної безпеки, що виконує такі основні функції:

– організація санкціонованого доступу до даних;

– моніторинг небезпечних подій;

– управління властивостями користувача МІС;

– ведення журналів безпеки.

Дані обчислювальної техніки, канали зв’язку для передачі персональних даних, використовувані при роботі телемедичної системи, повинні бути захищені організаційними заходами і засобами захисту інформації, які пройшли процедуру оцінки відповідності вимогам законодавства України в області забезпечення безпеки інформації.

Медичні документи в телемедичної системі можуть підписуватися з використанням посиленого кваліфікованого електронного підпису.

Обласна телемедична система розрахована на роботу як на захищених, так і по відкритих каналах зв’язку, включаючи мережу Інтернет. Для захисту інформації, що передається по відкритих каналах зв’язку, що підтримує протоколи TCP / IP, використовується сімейство апаратних і програмних продуктів VPN.

Стандарти оснащення ТКП/ТКК засобами захисту інформації і каналів зв’язку наведені в додатку .

При проведенні екстреної телемедичної консультації допускається передача персональних даних пацієнта по відкритих каналах зв’язку без письмової згоди пацієнта, якщо отримання згоди суб’єкта персональних даних неможливо.

Етико-деонтологічні норми дотримання принципу інформованої згоди

– перед проведенням телеконсультування лікар повинен дати пацієнту чіткі і зрозумілі пояснення, що стосуються необхідності телемедичної консультації з урахуванням можливостей і обмежень;

– рекомендовано отримувати письмову згоду пацієнта на відправку по телекомунікаційний каналам зв’язку інформацію про стан його здоров’я.

Дотримання конфіденційності та анонімності:

– технічний персонал, що обробляє і пересилає інформацію в телемедичної системі, повинен давати підписку про виконання норм, вимог і правил організаційного і технічного характеру, що стосуються захисту і нерозголошення оброблюваної інформації;

– при пересиланні (розміщенні в комп'ютерній мережі) медичної інформації необхідно дотримуватися принципу лікарської таємниці;

– всі персональні комп'ютери телемедичних пунктів та кабінетів повинні мати авторизований доступ (паролі);

– папки і локальні диски, що містять матеріали телеконсультування, повинні бути закриті для доступу в локальній мережі.

Дотримання юридичних норм:

– відповідальність за зміни в стані здоров'я пацієнта, які настали через використання (невикористання) рекомендацій консультанта, несе лікуючий лікар;

– необхідне ретельне протоколювання всіх телемедичних процедур, створення резервних і "твердих" копій;

– бажано використання цифрового підпису для ідентифікації учасника телеконсультування та припинення доступу до електронних даних про пацієнта з боку третіх осіб.

3.Принципи безпеки

Існує три основних принципи безпеки для будь-яких видів управління безпекою: доступність, цілісність і конфіденційність. Кожен механізм захисту (або управління) реалізує як мінімум один з цих принципів. Спеціаліст з безпеки повинен розуміти всі можливі способи реалізації цих принципів.

Доступність. Інформація, системи і ресурси повинні бути доступні користувачам в потрібний їм час, бо це необхідно для виконання ними своїх обов'язків. Відсутність доступу до інформації може зробити істотний негативний вплив на продуктивність роботи користувачів.

Слід застосовувати механізми забезпечення стійкості до відмов і відновлення для забезпечення безперервної доступності ресурсів. Інформація має різні атрибути, такі як точність, актуальність, оперативність і таємність.

Цілісність. Інформація повинна бути точною, повною і захищеною від несанкціонованих змін. Механізми безпеки, що забезпечують цілісність інформації, повинні повідомляти користувачів або адміністраторів про факти незаконних змін.

Конфіденційність. Інформація повинна бути захищена від несанкціонованого розкриття неуповноваженими особами, програмами або процесами. Одна інформація може бути більш критична, ніж інша інформація, тому вона вимагає більш високого рівня конфіденційності. У зв'язку з цим дані повинні бути класифіковані. Слід застосовувати механізми управління, які вказують, хто має доступ до даних і що може робити з ними,

отримавши доступ. Ця діяльність повинна контролюватися і постійно відслідковуватися. Прикладом конфіденційної інформації можуть бути медичні записи, фінансові рахунки, вихідні тексти програм, військові тактичні плани. Деякі механізми безпеки забезпечують конфіденційність засобами шифрування, управління логічним і фізичним доступом, управління потоками трафіку, використанням безпечних протоколів і т.п.

Ідентифікація, аутентифікація, авторизація та звітність

Користувачеві, щоб отримати доступ до ресурсу, потрібно спочатку підтвердити, що він є тим, за кого себе видає, має необхідні повноваження, а також права і привілеї для виконання дій, які він запросив. Тільки при успішному виконанні всіх цих кроків користувачеві повинен надаватися доступ до ресурсів. Крім того, необхідно відстежувати дії користувачів, використовуючи для цього засоби ведення обліку. Ідентифікація – це метод перевірки, який підтверджує, що суб'єкт (користувач, програма або процес) – той, за кого себе видає. Ідентифікація може здійснюватися, наприклад, з використанням імені користувача або номера рахунку.

Для проходження аутентифікації суб'єкт звичайно повинен надати другу частину облікових даних, наприклад, пароль, парольну фразу, криптографічний ключ, PIN-код, біометричний атрибут або токен. Ці дві частини облікових даних порівнюються з попередньо збереженою інформацією про суб'єкта і, якщо вони збігаються, автентифікація вважається успішною. Далі система перевіряє матрицю контролю доступу або порівнює мітки безпеки для перевірки, що суб'єкт дійсно може використовувати ресурс і виконувати запитані дії з ним. Якщо система визначає, що суб'єкт може отримати доступ до ресурсу, вона авторизує його.

Хоча ідентифікація, автентифікація, авторизація та підзвітність тісно пов'язані між собою, кожен елемент має різні функції, які реалізують певні вимоги в процесі управління доступом. Користувач може бути успішно ідентифікований та автентифікований для доступу до мережі, але він може не мати дозволу на доступ до файлів на файловому сервері. Або навпаки, користувачеві може бути наданий доступ до файлів на файловому сервері, але поки він не пройшов успішно процедури ідентифікації і автентифікації, ці файли йому недоступні.

Суб'єкт повинен нести відповідальність за всі дії, вчинені від його імені в системі або домені. Єдиним способом забезпечення звітності є належна ідентифікація суб'єкта і запис всіх його дій.

Логічне керування доступом – це інструмент, який використовується для ідентифікації, автентифікації, авторизації та звітності. Це реалізується у вигляді програмних компонентів, що виконують функції управління доступом до систем, програм, процесів та інформації. Логічне керування доступом може бути вбудовано в операційну систему, застосування, додаткові пакети безпеки, бази даних або системи управління телекомунікаціями. Достатньо складно синхронізувати всі механізми управління доступом, врахувавши при цьому всі можливі вразливості і не

зашкодивши продуктивності. У процесі автентифікації повинна бути перевірена особистість людини.

Автентифікація, як правило, включає в себе два етапи: введення публічної інформації (ім'я користувача, ідентифікатор, номер рахунку тощо), а потім введення секретної інформації (постійний пароль, смарт-картка, одноразовий пароль, PIN-код, електронно-цифровий підпис і т.п.).

Введення публічної інформації – це ідентифікація, а введення секретної інформації – автентифікація. Кожен метод, використовуваний для ідентифікації і автентифікації, має свої плюси і мінуси. Слід проводити належну оцінку методів ідентифікації і автентифікації для вибору правильного механізму для наявної середовища.

Загрози інформаційної безпеки

Розгляд можливих загроз інформаційної безпеки проводиться з метою визначення повного набору вимог до розроблюваної системи захисту. Зазвичай під загрозою (в загальному сенсі) розуміють потенційно можливу подію (вплив, процес або явище), яка може зробити небажаний вплив на систему, а також на інформацію, що зберігається в ній. Далі під загрозою безпеці інформаційної системи (ІС) будемо розуміти можливість впливу на ІС, яка прямо або непрямо може завдати їй шкоди.

В даний час відомий досить великий перелік загроз безпеки ІС, що містить сотні позицій. Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту ІС.

Крім виявлення можливих загроз, доцільно проведення аналізу цих загроз на основі їх класифікації за рядом ознак. Кожна з ознак класифікації відбиває одну із узагальнених вимог до системи захисту. Загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати вимогу, що відображає ця ознака. Необхідність класифікації загроз безпеки ІС обумовлена тим, що інформація, яка зберігається та оброблюється в сучасних ІС, піддана впливу надзвичайно великого числа факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тому для системи, яка захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Прийнято вважати, що, незалежно від конкретних видів загроз і їх проблемно-орієнтованої класифікації, ІС задовольняє потреби експлуатуючих її осіб, якщо забезпечуються наступні важливі властивості інформації та систем її обробки: доступність, цілісність і конфіденційність інформації. Іншими словами, інформаційна безпека ІС забезпечена у разі, якщо для інформаційних ресурсів у системі підтримуються певні рівні:

- доступності (можливості за розумний час отримати необхідну інформацію);
- цілісності (неможливості несанкціонованої або випадкової модифікації інформації);

- конфіденційності (неможливості несанкціонованого отримання інформації).

Відповідно, для автоматизованих **інформаційних систем загрози слід класифікувати насамперед по аспекту інформаційної безпеки (доступність, цілісність, конфіденційність),** проти якого вони спрямовані в першу чергу:

- загрози порушення доступності (відмова в обслуговуванні), спрямовані на створення таких ситуацій, коли певні дії або блокують доступ до деяких ресурсів ІС, або знижують її працездатність. Наприклад, якщо один користувач системи запитує доступ до деякої служби, а інший виконує дії по блокуванню цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним або тимчасовим;
- загрози порушення цілісності інформації, що зберігається в комп'ютерній системі чи переданої по каналу зв'язку, які спрямовані на її зміну або спотворення, що приводить до порушення її якості або повного знищення.

Цілісність інформації може бути порушена навмисно зловмисником, а також в результаті об'єктивних впливів з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації – комп'ютерних мереж і систем телекомунікацій. Навмисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція якої-небудь бази даних);

- загрози порушення конфіденційності, спрямовані на розголошення конфіденційної або секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ. У термінах комп'ютерної безпеки загроза порушення конфіденційності має місце щоразу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі чи переданої від однієї системи до іншої. Дані види загроз можна вважати первинними, або безпосередніми, оскільки їх реалізація веде до безпосередньої дії на захищену інформацію.

Класифікація можливих загроз безпеки ІС може бути проведена також по ряду інших ознак.

- *За природою виникнення розрізняють*:

Природні загрози, викликані впливами на ІС об'єктивних фізичних процесів або стихійних природних явищ;

Штучні загрози безпеки ІС, викликані діяльністю людини.

- *За ступенем навмисності прояву розрізняють*:

Загрози, викликані помилками або халатністю персоналу, наприклад некомпетентного використання засобів захисту; введення помилкових даних, тощо;

Загрози навмисної дії, наприклад дії зловмисників.

• *По безпосередньому джерелу загроз*.

Джерелами загроз можуть бути:

Природне середовище, наприклад стихійні лиха, магнітні бурі, тощо;

Людина, наприклад вербування шляхом підкупу персоналу, розголошення конфіденційних даних, тощо;

Санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі операційної системи;

Несанкціоновані програмно-апаратні засоби, наприклад зараження комп'ютера вірусами з деструктивними функціями.

• *За положенням джерела загроз.* Джерело загроз може бути розташоване:

поза контрольованою зоною ІС, наприклад перехоплення даних, переданих по каналах зв'язку, перехоплення електромагнітних, акустичних та інших випромінювань пристроїв;

в межах контрольованої зони ІС, наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації тощо; безпосередньо в ІС, наприклад некоректне використання ресурсів ІС.

• *За ступенем залежності від активності ІС.* Загрози проявляються:

незалежно від активності ІС, наприклад зламування шифрів криптозахисту інформації;

тільки в процесі обробки даних, наприклад загрози виконання і розповсюдження програмних вірусів.

• *За ступенем впливу на ІС розрізняють*:

пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті ІС, наприклад загроза копіювання секретних даних;

активні загрози, які при впливі вносять зміни в структуру та зміст ІС, наприклад впровадження троянських коней і вірусів.

• *По етапах доступу користувачів або програм до ресурсів ІС розрізняють:*

загрози, які проявляються на етапі доступудо ресурсів ІС, наприклад загрози несанкціонованого доступу в ІС;

загрози, які проявляються після дозволу доступу до ресурсів ІС, наприклад загрози несанкціонованого або некоректного використання ресурсів ІС.

• *За способом доступу до ресурсів ІС розрізняють*:

загрози з використанням стандартного шляху доступу до ресурсів ІС, наприклад незаконне отримання паролів і інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;

загрози з використанням прихованого нестандартного шляху доступу до ресурсів ІС, наприклад несанкціонований доступ до ресурсів ІС шляхом використання не документованих можливостей ОС.

• *За поточним місцем розташування інформації, що зберігається і оброблюваної в ІС, розрізняють:*

загрози доступу до інформації на зовнішніх запам'ятовуючих пристроях, наприклад несанкціоноване копіювання секретної інформації з жорсткого диску;

загрози доступу до інформації в оперативній пам'яті, наприклад читання залишкової інформації з оперативної пам'яті;

доступ до системної області оперативної пам'яті з боку прикладних програм;

загрози доступу до інформації, що циркулює в лініях зв'язку, наприклад незаконне підключення до ліній зв'язку з подальшим введенням помилкових повідомлень або модифікацією переданих повідомлень;

незаконне підключення до ліній зв'язку з метою прямої підміни легального користувача з подальшим введенням дезінформації та нав'язуванням помилкових повідомлень;

загрози доступу до інформації, яка відображається на терміналі або що друкується на принтері, наприклад запис відображуваної інформації на приховану відеокамеру.

Як вже зазначалося, небезпечний вплив на ІС поділяють на випадковий і навмисний. Аналіз досвіду проектування, виготовлення і експлуатації ІС показує, що інформація піддається різним випадковим впливам на всіх етапах циклу життя і функціонування ІС.

Причинами випадкових впливів при експлуатації ІС можуть бути:

- аварійні ситуації через стихійні лиха та відключення електроживлення;
- відмови і збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу і користувачів;
- перешкоди в лініях зв'язку через вплив зовнішнього середовища.

Помилки в програмному забезпеченні (ПЗ) є поширеним видом комп'ютерних порушень. Програмне забезпечення серверів, робочих станцій, маршрутизаторів написане людьми, тому воно практично завжди містить помилки. Чим вища складність подібного програмного забезпечення, тим більша вірогідність виявлення в ньому помилок і вразливостей. Більшість з них не представляють ніякої небезпеки, деякі ж можуть призвести до серйозних наслідків, таких як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів (використання комп'ютера як плацдарму для атаки та інше). Зазвичай подібні помилки усуваються за допомогою пакетів оновлень, які регулярно випускаються виробником ПЗ. Своєчасна установка таких пакетів є необхідною умовою безпеки інформації.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. В якості порушника можуть виступати службовець, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом

(хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися будь-якою ціною тощо.

Виходячи з можливості виникнення найбільш небезпечної ситуації, обумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушнику відома інформація про принципи роботи системи;
- порушник вибере найбільш слабку ланку в захисті.

До таких порушників належать, зокрема, інсайдери. Інсайдер – це людина, допущена до роботи з інформацією, яка призначена для строго обмеженого кола осіб. Використовуючи своє становище, інсайдери крадуть інформацію. Вони можуть передавати її по електронній пошті, копіювати на різні USB-пристрої і КПК, записувати в ноутбуки, роздруковувати і виносити на папері, викладати на всілякі файлообмінні ресурси.

Найбільш поширеним і різноманітним видом комп'ютерних порушень є несанкціонований доступ (НСД). Суть НСД полягає в отриманні користувачем (порушником) доступу до об'єкта в порушення правил розмежування доступу, встановлених відповідно до прийнятої в організації політики безпеки. НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректного встановлення та налаштування. НСД може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Перелічимо основні канали несанкціонованого доступу, через які порушник може отримати доступ до компонентів ІС і здійснити розкрадання, модифікацію та/або руйнування інформації:

- штатні канали доступу до інформації (термінали користувачів, оператора, адміністратора системи; засоби відображення і документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;
- технологічні пульти управління;
- лінії зв'язку між апаратними засобами ІС;
- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення і заземлення та ін.

З усього розмаїття способів і прийомів несанкціонованого доступу варто зупинитись на наступних поширених і пов'язаних між собою порушеннях:

- перехоплення паролів;
- маскарад;
- незаконне використання привілеїв;
- шкідливі програми.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача увійти в систему, програма-перехоплювач імітує на екрані дисплея введення імені та паролю користувача, які відразу пересилаються власнику програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач припускає, що допустив помилку при введенні пароля. Він повторює введення і отримує доступ в систему. Власник програми-перехоплювача, що отримав ім'я і пароль законного користувача, може тепер використовувати їх у своїх цілях. Існують і інші способи перехоплення паролів.

Маскарад – це виконання будь-яких дій одним користувачем від імені іншого користувача, що володіє відповідними повноваженнями. Метою маскараду є приписування будь-яких дій іншому користувачеві або при-присвоєнні повноважень і привілеїв іншого користувача. Прикладами реалізації маскараду є:

- вхід в систему під ім'ям і паролем іншого користувача (цьому маскараду передує перехоплення пароля);
- передача повідомлень у мережі від імені іншого користувача.

Маскарад особливо небезпечний в банківських системах електронних платежів, де неправильна ідентифікація клієнта через маскарад зловмисника може призвести до великих збитків законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожен користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад, за допомогою маскараду, призводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або при наявності помилок у системі захисту, або через недбалість адміністратора при управлінні системою і призначення привілеїв.

Шкідливі програми. До таких програм відносяться комп'ютерні віруси, мережні черв'яки, програма «троянський кінь». Особливо вразливі до цих програм робочі станції кінцевих користувачів. Дамо коротку характеристику цих поширених загроз безпеки ІС.

Комп'ютерний вірус являє собою своєрідне явище, що виникло в процесі розвитку комп'ютерної та інформаційної техніки. Суть цього явища полягає в тому, що програми-віруси мають ряд особливостей, властивих живим організмам, вони народжуються, розмножуються і помирають.

Термін «вірус» у застосуванні до комп'ютерів запропонував Фред Коен з університету Південної Каліфорнії. Історично перше визначення вірусу було дано Ф. Коеном: «Комп'ютерний вірус – це програма, яка може заражати інші програми, модифікуючи їх допомогою включення в них своєї, можливо, зміненої копії, причому остання зберігає здатність до подальшого розмноження». Комп'ютерні віруси завдають шкоди системі за рахунок швидкого розмноження і руйнування середовища проживання.

Мережний черв’як є різновидом програми-вірусу, який поширюється глобальною мережею. «Троянський кінь» являє собою програму, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи і деструктивних результатів. Аналогія такої програми з давньогрецьким троянським конем цілком виправдана, тому що в обох випадках оболонка, яка не викликає підозру, таїть серйозну загрозу. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, яке повинне захищатися від несанкціонованого доступу. Слід зазначити, що троянські коні, комп’ютерні віруси і мережні черв’яки відносяться до вельми небезпечних загроз ІС. Особливістю сучасних шкідливих програм є їхня орієнтація на конкретне прикладне ПЗ, що стало стандартом де-факто для більшості користувачів, в першу чергу це Microsoft Internet Explorer і Microsoft Outlook. Масове створення вірусів під продукти Microsoft пояснюється не тільки низьким рівнем безпеки і надійності програм, важливу роль грає глобальне поширення цих продуктів.

Автори шкідливого програмного забезпечення все активніше починають досліджувати «дірки» в популярних СУБД, в пов’язаних з ними ПЗ і корпоративних бізнес-застосуваннях, побудованих на базі цих систем.

Шкідливі програми постійно еволюціонують, основною тенденцією їх розвитку є поліморфізм. Сьогодні вже досить складно провести межу між вірусом, черв’яком і троянською програмою – вони використовують практично одні й ті ж механізми, невелика різниця полягає лише в ступені цього використання. Структура шкідливого програмного забезпечення стала сьогодні настільки уніфікованою, що, наприклад, відрізнити поштовий вірус від черв’яка з деструктивними функціями практично неможливо. Навіть у троянських програмах з’явилася функція реплікації (як один із засобів протидії антивірусним засобам), так що при бажанні їх цілком можна назвати вірусами (з механізмом поширення у вигляді маскування під прикладні програми).

Для захисту від шкідливих програм необхідно застосування низки заходів:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування придбаних програмних засобів;
- контроль цілісності виконуваних файлів і системних областей;
- створення замкнутого середовища виконання програм.

Боротьба з вірусами, черв’яками і троянськими кіньми ведеться за допомогою ефективного антивірусного програмного забезпечення, що працює на рівні користувача і на рівні мережі. У міру появи нових вірусів, черв’яків і троянських коней потрібно оновлювати бази даних антивірусних засобів і застосувань. Як уже зазначалося, загрози порушення доступності, цілісності і конфіденційності інформації є первинними або безпосередніми, оскільки реалізація цих загроз веде до безпосередньої дії на інформацію, яка захищається.

Для сучасних інформаційних технологій підсистеми захисту є невід'ємною частиною ІС обробки інформації. Атакуюча сторона повинна здолати цю підсистему захисту, щоб порушити, наприклад, конфіденційність ІС. Однак потрібно усвідомлювати, що не існує абсолютно стійкою системи захисту, питання лише в часі і засобах, потрібних на її подолання. Подолання захисту також являє собою загрозу, тому для захищених систем можна розглядати четвертий вид загрози – загрозу розкриття параметрів ІС, що включає в себе підсистему захисту. На практиці будь-який проведений захід випереджається етапом розвідки, в ході якого визначаються основні параметри системи, її характеристики тощо. Результатом цього етапу є уточнення поставленого завдання, а також вибір найбільш оптимального технічного засобу. Загрозу розкриття параметрів ІС можна вважати опосередкованою. Наслідки її реалізації не заподіюють якого-небудь збитку оброблюваній інформації, але дають можливість реалізувати первинні або безпосередні загрози, перераховані вище.

Типи атак на інформаційні системи

Стрімке зростання популярності Інтернет-технологій супроводжується зростанням серйозних загроз розголошення персональних даних, критично важливих корпоративних ресурсів, державних таємниць тощо. Кожен день зловмисники піддають загрозам мережні інформаційні ресурси, намагаючись отримати до них доступ за допомогою спеціальних атак. Ці атаки стають все більш витонченими по впливу і нескладними у виконанні. Цьому сприяють два основні чинники.

По-перше, це повсюдне проникнення мережі Інтернет. Сьогодні до цієї мережі підключені мільйони комп'ютерів. Багато мільйонів комп'ютерів будуть підключені до мережі Інтернет в найближчому майбутньому, тому ймовірність доступу зловмисників до вразливих комп'ютерів і комп'ютерних мереж постійно зростає. Крім того, широке поширення мережі Інтернет дозволяє зловмисникам обмінюватися інформацією в глобальному масштабі.

По-друге, це загальне поширення простих у використанні операційних систем і середовищ розробки. Цей фактор різко знижує вимоги до рівня знань зловмисника. Раніше від зловмисника були потрібні хороші знання і навички програмування, щоб створювати і поширювати шкідливі програми. Тепер для того, щоб отримати доступ до чужого комп'ютера, потрібно просто знати IP-адресу потрібного сайту, а для проведення атаки досить клацнути мишею. Проблеми забезпечення інформаційної безпеки в корпоративних комп'ютерних мережах обумовлені загрозами безпеці для локальних робочих станцій, локальних мереж і атаками на корпоративні мережі, що мають вихід в загальнодоступні мережі передачі даних.

Мережні атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються великою складністю. Інші – здатний здійснити звичайний оператор, навіть не припускаючи, які наслідки може мати його діяльність.

Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі:

- порушення конфіденційності переданої інформації;
- порушення цілісності та достовірності інформації, що передається;
- порушення працездатності системи в цілому або окремих її частин.

З точки зору безпеки розподілені системи характеризуються насамперед наявністю віддалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних і порушник може не тільки проводити пасивне прослуховування переданої інформації, але і модифікувати переданий трафік (активний вплив). І якщо активний вплив на трафік може бути зафіксований, то пасивний вплив практично не піддається виявленню. Але оскільки в ході функціонування розподілених систем обмін службовою інформацією між компонентами системи здійснюється теж по відкритих каналах передачі даних, то службова інформація стає таким же об'єктом атаки, як і дані користувача. **Атаки доступу**

Атака доступу – це спроба отримання зловмисником інформації, на ознайомлення з якою у нього немає дозволу. Атака доступу спрямована на порушення конфіденційності інформації.

Підслуховування (Sniffing). Здебільшого дані передаються по комп'ютерним мережам в незахищеному форматі (відкритим текстом), що дозволяє зловмисникові, що отримав доступ до ліній передачі даних в мережі, підслуховувати або зчитувати трафік. Для підслуховування у комп'ютерних мережах використовують сніфер. Сніфер пакетів являє собою прикладну програму, яка перехоплює всі мережні пакети, що передаються через певний сегмент. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак через те, що деякі мережні застосування передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніферу можна дізнатися корисну, а іноді, і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Запобігти загрозі сніфінгу пакетів можна за допомогою наступних заходів і засобів:

застосування для автентифікації одноразових паролів;

установка апаратних або програмних засобів, які розпізнають сніфери;

застосування криптографічного захисту каналів зв'язку.

Перехоплення (Hijacking). На відміну від підслуховування, перехоплення – це активна атака. Зловмисник перехоплює інформацію в процесі її передачі до місця призначення. Перехоплення імен і паролів створює велику небезпеку, оскільки користувачі часто застосовують одні й ті ж логін та пароль для безлічі застосувань і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і застосувань. Якщо застосування працює в режимі клієнт/сервер, а автентифікаційні дані передаються по мережі у відкритому текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів. В найгіршому випадку зловмисник отримує доступ до ресурсу користувача на системному рівні і з його

допомогою створює атрибути нового користувача, які можна в будь-який момент застосувати для доступу в мережу і до її ресурсів.

Перехоплення сеансу (Session Hijacking). По закінченні початкової процедури автентифікації з'єднання, встановлене законним користувачем, наприклад, з поштовим сервером, перемикається зловмисником на новий вузол, а вихідному серверу надається команда розірвати з'єднання. В результаті «співрозмовник» законного користувача виявляється непомітно підміненим. Після отримання доступу до мережі у атакуючого зловмисника з'являються великі можливості:

- він може посилати некоректні дані застосуванням і мережним службам, що призводить до їх аварійного завершення або неправильного функціонування;
- він може також наповнити комп'ютер або всю мережу трафіком, поки не відбудеться зупинка системи у зв'язку з перевантаженням;
- нарешті, атакуючий може блокувати трафік, що призведе до втрати доступу авторизованих користувачів до мережних ресурсів.

Атаки модифікації

Атака модифікації – це спроба неправомірної зміни інформації. Така атака можлива скрізь, де існує або передається інформація; вона спрямована на порушення цілісності інформації.

Зміна даних. Зловмисник, отримавши можливість прочитати чужі дані, зможе зробити і наступний крок – змінити їх. Дані в пакеті можуть бути змінені, навіть якщо зловмисник нічого не знає, ні про відправника, ні про одержувача.

Додавання даних. Інший тип атаки – додавання нових даних, наприклад, в інформацію про історію минулих періодів.

Видалення даних. Атака видалення означає переміщення існуючих даних, наприклад анулювання запису про операції з балансового звіту банку, в результаті чого зняті з рахунку грошові кошти залишаються на ньому.

Атаки типу «відмова в обслуговуванні» Атака «відмова в обслуговуванні» (Denial-of-Service, DoS) відрізняється від атак інших типів. Вона не націлена на отримання доступу до мережі або витягу з цієї мережі будь-якої інформації. DoS-атака робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. По суті, ця атака позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації. Більшість DoS-атак спирається на загальні слабкості системної архітектури. У разі використання деяких серверних застосувань (таких, як веб- або FTP-сервер) DoS-атаки можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих застосувань, і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів.

В ході DoS-атак можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP (Internet Control Message Protocol). DoS-атакам важко запобігти, оскільки для цього потрібна координація дій з провайдером. Якщо трафік, призначений для переповнення мережі, не зупинити у

провайдера, то на вході в мережу це зробити вже не можливо, тому що вся смуга пропускання буде зайнята. Якщо атака цього типу проводиться одночасно через безліч пристроїв, то говорять про розподілену атаку «відмова в обслуговуванні»(DDoS, Distributed DoS). Простота реалізації DoS-атак і величезна шкода, заподіяна ними організаціям і користувачам, притягують до цих атак пильну увагу адміністраторів мережної безпеки.

Відмова в доступі до інформації. В результаті DoS-атаки, спрямованої проти інформації, остання стає непридатною для використання. Інформація знищується, спотворюється або переноситься в недоступне місце.

Відмова в доступі до застосувань. Інший тип DoS-атак спрямований на застосування, що обробляють або відображають інформацію, або на комп'ютерну систему, в якій ці застосування виконуються. У разі успіху подібної атаки рішення задач, які виконуються за допомогою такого застосування, стає неможливим.

Відмова в доступі до системи. Загальний тип DoS-атак ставить своєю метою виведення з ладу комп'ютерної системи, в результаті чого сама система, встановлені на ній застосування і вся збережена інформація стають недоступними.

Відмова в доступі до засобів зв'язку. Метою атаки є комунікаційне середовище. Цілісність комп'ютерної системи і інформації не порушується, однак відсутність засобів зв'язку позбавляє користувачів доступу до цих ресурсів.

Комбіновані атаки

Комбінована атака полягає в застосуванні зловмисником декількох взаємно пов'язаних дій для досягнення своєї мети.

Підміна довіреного суб'єкту. Більша частина мереж і операційних систем використовують IP-адресу комп'ютера для того, щоб визначати, чи той це адресат, який потрібен. У деяких випадках можливе некоректне присвоєння IP-адреси (підміна IP-адреси відправника іншою адресою) – такий спосіб атаки називають фальсифікацією адреси або IP-спуфінгом (IP-spoofing). IP-спуфінг має місце, коли зловмисник, що знаходиться всередині корпоративної мережі або за її межами, видає себе за законного користувача. Зловмисник може скористатися його IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або авторизованою зовнішньою адресою, якій дозволяється доступ до певних ресурсів мережі. Зловмисник може також використовувати спеціальні програми, які формують IP-пакети таким чином, щоб вони виглядали як вихідні з дозволених внутрішніх адрес корпоративної мережі.

Атаки IP-спуфінга часто є відправною точкою для інших атак. Класичним прикладом є атака типу «відмова в обслуговуванні» (DoS), яка починається з чужої адреси, що приховує справжню особу зловмисника. Зазвичай IP-спуфінг обмежується вставкою неправдивої інформації або шкідливих команд у звичайний потік даних, що передаються між клієнтським і серверним застосуваннями або по каналу зв'язку між одноранговими пристроями.

Загрозу спуфінга можна послабити (але не усунути) за допомогою наступних заходів:

правильне налаштування управління доступом із зовнішньої мережі;

припинення спроб спуфінга чужих мереж користувачами мережі. Потрібно мати на увазі наступне: IP-спуфінг може бути здійснений за умови, що автентифікація користувачів проходить на базі IP-адрес, тому введення додаткових методів автентифікації користувачів (на основі одноразових паролів або інших методів криптографії) дозволяє запобігти атаки IP-спуфінга.

Посередництво. Атака типу «посередництво» передбачає активне підслуховування, перехоплення даних, які передаються, невидимим проміжним вузлом і управління ними. Коли комп'ютери взаємодіють на мережному рівні, вони не завжди можуть визначити, з ким саме вони обмінюються даними. Посередництво в обміні незашифрованими ключами (атака Man-in-the-Middle – «людина-в-середині»).

Для проведення атаки «людина-в-середині» зловмиснику потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера ISP в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніфери пакетів, транспортні протоколи та протоколи маршрутизації.

У більш загальному випадку атаки «людина-в-середині» проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережних ресурсів, для аналізу трафіку і отримання інформації про мережі та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережні сесії.

Ефективно боротися з атаками типу «людина-в-середині» можна тільки за допомогою криптографії. Для протидії атакам цього типу використовується інфраструктура відкритих ключівPKI (Public Key Infrastructure).

Атака експлоїта. Експлоїт (exploit – експлуатувати) – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та застосовуються для проведення атаки на комп'ютерну систему. Метою атаки може бути як захоплення контролю над системою, так і порушення її функціонування (DoS-атака). Залежно від методу отримання доступу до вразливого програмного забезпечення, експлоїти поділяються на віддалені і локальні:

- віддалений експлоїт працює через мережу і використовує вразливість в захисті без якого-небудь попереднього доступу до вразливої системи;
- локальний експлоїт запускається безпосередньо у вразливій системі, вимагаючи попереднього доступу до неї.

Зазвичай використовується для отримання зловмисником прав суперкористувача. Атака експлоїта може бути спрямована на різні

компоненти комп'ютерної системи – серверні застосування, клієнтські програми або модулі операційної системи.

Парольні атаки. Метою цих атак є заволодіння паролем і логіном законного користувача. Зловмисники можуть проводити парольні атаки, використовуючи такі методи, як:

- підміна IP-адреси (IP-спуфінг);
- підслуховування (сніфінг);
- простий перебір.

Вгадування ключа. Криптографічний ключ являє собою код або число, необхідне для розшифрування захищеної інформації. Хоча дізнатися ключ доступу важко і такі спроби вимагають великих витрат ресурсів, тим не менш, це можливо. Зокрема, для визначення значення ключа може бути використана спеціальна програма, яка реалізує метод повного перебору. Ключ, до якого отримує доступ атакуючий, називається скомпрометованим. Атакуючий використовує скомпрометований ключ для отримання доступу до захищених даними без відома відправника і одержувача. Ключ дає можливість розшифровувати і редагувати дані. **Атаки на рівні застосувань.** Ці атаки можуть проводитися декількома способами. Найпоширеніший з них полягає у використанні відомих вразливостей серверного програмного забезпечення (FTP, HTTP, веб-сервера). Головна проблема з атаками на рівні застосувань полягає в тому, що зловмисники часто користуються портами, яким дозволено прохід через мережні екрани. Відомості про атаки на рівні застосувань широко публікуються, щоб дати можливість адміністраторам вирішити проблему за допомогою корекційних модулів (патчів). На жаль, багато зловмисників також мають доступ до цих відомостей, що дозволяє їм вчитися. Неможливо повністю виключити атаки на рівні застосувань. Зловмисники постійно відкривають і публікують на своїх сайтах в мережі Інтернет нові вразливі місця прикладних програм. Тут важливо здійснювати хороше системне адміністрування.

Щоб зменшити вразливість від атак цього типу, можна зробити наступні заходи:

- аналізувати лог-файли операційних систем і мережні лог-файли за допомогою спеціальних аналітичних програм;
- відстежувати дані CERT про слабкі місця прикладних програм;
- користуватися самими свіжими версіями операційних систем і застосувань і останніми корекційними модулями (патчами);
- використовувати системи виявлення вторгнень IDS (Intrusion Detection Systems).

Аналіз мережного трафіку. Метою атак подібного типу є прослуховування каналів зв'язку і аналіз даних, які передаються, та службової інформації з метою вивчення топології мережі та архітектури побудови системи, отримання критичної інформації користувачів (наприклад, паролів користувачів або номерів кредитних карт, що передаються у відкритому вигляді). Атакам цього типу схильні такі

протоколи, як FTP і Telnet, особливістю яких є те, що ім'я та пароль користувача передаються в рамках цих протоколів у відкритому вигляді.

Мережна розвідка.

Мережна розвідка – це збір інформації про мережу за допомогою загальнодоступних даних і застосувань. При підготовці атаки проти якої-небудь мережі зловмисник, як правило, намагається отримати про неї якомога більше інформації.

Мережна розвідка проводиться у формі запитів DNS, ICMP-тестування (Ping Sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цьому домену належать. ICMP-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які вузли реально працюють в цій мережі. Отримавши список вузлів, зловмисники використовують засоби сканування портів, щоб скласти повний список сервісів, які підтримуються цими вузлами. В результаті отримується інформація, яку можна використовувати для злому.

Зловживання довірою. Даний тип дій не є атакою в повному сенсі цього слова. Він являє собою зловмисне використання відносин довіри, що існують в мережі. Типовим прикладом такого зловживання є ситуація в периферійній частині корпоративної мережі. У цьому сегменті зазвичай розташовуються сервери DNS, SMTP і HTTP. Оскільки всі вони належать до одного і того ж сегменту, злом одного з них призводить до злому і всіх інших, так як ці сервери довіряють іншим системам своєї мережі. Ризик зловживання довірою можна знизити за рахунок більш жорсткого контролю рівнів довіри в межах своєї мережі. Системи, розташовані з зовнішнього боку мережного екрану, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених мережним екраном. Відносини довіри повинні обмежуватися певними протоколами і по можливості автентифікуватися не тільки по IP-адресами, але і за іншими параметрами.

Фішинг (Phishing). Фішинг є відносно новим видом Інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків, PIN-кодів та іншої конфіденційної інформації, що дає доступ до грошей користувача. Фішинг не використовує технічні недоліки програмного забезпечення, а легковірність користувачів мережі Інтернет. Сам термін phishing, співзвучний з fishing (риболовля), розшифровується як password harvesting fishing – виуджування пароля. Дійсно, фішинг дуже схожий на рибну ловлю. Зловмисник закидає в Інтернет приманку і «виловлює» всіх «рибок» – користувачів мережі Інтернет, які клюнуть на цю приманку. Зловмисник створює практично точну копію сайту обраного банку (електронної платіжної системи, аукціону тощо). Потім за допомогою спам-технології по електронній пошті розсилається лист, складений таким чином, щоб бути максимально схожим на даний лист від обраного банку. При складанні листа використовуються логотипи банку, імена і прізвища реальних керівників банку. В такому листі, як правило, повідомляється про те, що із-за зміни програмного забезпечення в системі інтернет-банкінгу

користувачеві необхідно підтвердити або змінити свої облікові дані. В якості причини для зміни даних можуть бути названі вихід з ладу ПЗ банку або ж напад зловмисників. Наявність правдоподібної легенди, що спонукає користувача до необхідних дій – неодмінна складова успіху шахраїв-фішерів. У всіх випадках мета таких листів одна – змусити користувача клацнути по наведеним посиланням, а потім ввести свої конфіденційні дані (пароль, номер рахунку, PIN-код) на фальшивому сайті банку (електронної платіжної системи, аукціону). Зайшовши на фальшивий сайт, користувач вводить у відповідні рядки свої конфіденційні дані, а далі аферисти отримують доступ в кращому випадку до його поштової скриньки, а в гіршому – до електронного рахунку. Успіху фішинг-афер сприяє низький рівень обізнаності користувачів про правила роботи компаній, від імені яких діють злочинці. Зокрема, близько 5% користувачів не знають простого факту: банки не розсилають листів з проханням підтвердити в онлайн номер своєї кредитної картки, її PIN-код. Основним захистом від фішингу поки залишаються спам-фільтри. На жаль, програмний інструментарій для захисту від фішингу володіє обмеженою ефективністю, оскільки зловмисники експлуатують в першу чергу не вразливості в ПЗ, а людську психологію. З'явилося поєднане з фішингом поняття – фармінг.

Фармінг (Pharming). Це ще один вид шахрайства, що ставить за мету отримати персональні дані користувачів, але не через пошту, а прямо через офіційні веб-сайти. Фармери замінюють на серверах DNS цифрові адреси легітимних веб-сайтів на підроблені, в результаті чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства ще небезпечніше, оскільки помітити підробку практично неможливо. Для захисту від фішингу та фармінгу розробляються технічні засоби безпеки, насамперед плагіни для популярних браузерів. Суть захисту полягає в блокуванні сайтів, що потрапили в чорні списки шахрайських ресурсів. Наступним кроком можуть стати системи генерації одноразових паролів для інтернет-доступу до банківських рахунків та записів в платіжних системах, повсюдне поширення додаткових рівнів захисту за рахунок комбінації введення пароля з використанням апаратного USB-ключа.

Застосування ботнетів. Ботнет (зомбі-мережа) – це мережа комп'ютерів, заражених шкідливою програмою, яка дозволяє кіберзлочинцям віддалено керувати зараженими машинами (кожною окремо, частиною комп'ютерів, що входять в мережу, або всією мережею цілком) без відома користувача. Такі програми називаються ботами. Ботнети володіють потужними обчислювальними ресурсами, є загрозливою кіберзброєю і хорошим способом заробляння грошей для зловмисників. При цьому зараженими машинами, що входять в мережу, господар ботнету може керувати звідки завгодно: з іншого міста, країни чи навіть з іншого континенту, а організація мережі Інтернет дозволяє робити це анонімно. Управління комп'ютером, який заражений ботом, може бути прямим і опосередкованим. У разі прямого управління зловмисник може встановити

зв’язок з інфікованим комп’ютером і керувати ним, використовуючи вбудовані в тіло програми-бота команди.

У випадку опосередкованого управління бот сам з’єднується з центром управління або іншими машинами в мережі, посилає запит і виконує отриману команду. У будь-якому випадку господар зараженої машини, як правило, навіть не підозрює про те, що вона використовується зловмисниками. Саме тому заражені шкідливою програмою-ботом комп’ютери, що знаходяться під таємним наглядом кіберзлочинців, називають ще зомбі-комп’ютерами, а мережа, до якої вони входять – зомбі-мережею. Найчастіше зомбі-машинами стають персональні комп’ютери домашніх користувачів. Ботнети можуть використовуватися зловмисниками для вирішення кримінальних завдань різного масштабу: від розсилки спаму до атак на державні мережі. Анонімний доступ в мережу. Зловмисники можуть звертатися до серверів в мережі Інтернет, використовуючи зомбі-машини, і від імені заражених машин здійснювати кіберзлочини, наприклад зламувати веб-сайти або переводити вкрадені грошові кошти.

Продаж і оренда ботнетів. Один з варіантів незаконного заробітку за допомогою ботнетів ґрунтується на здачі ботнету в оренду або продаж готової мережі. Створення ботнетів для продажу є окремим напрямком кіберзлочинного бізнесу. Крадіжка конфіденційних даних. Цей вид кримінальної діяльності постійно приваблює кіберзлочинців, а з допомогою ботнетів «улов» у вигляді різних паролів для доступу до електронної пошти, FTP-ресурсів, веб-сервісів) та інших конфіденційних даних користувачів збільшується в тисячі разів! Бот, яким заражені комп’ютери в зомбі-мережі, може завантажити іншу шкідливу програму, наприклад троянця, що краде паролі. У такому разі інфікованими троянською програмою виявляться всі комп’ютери, що входять в цю зомбі-мережу, і зловмисники зможуть отримати паролі зі всіх заражених машин. Вкрадені паролі перепродаються або використовуються, зокрема, для масового зараження веб-сторінок (наприклад, паролі для всіх знайдених FTP-акаунтів) з метою подальшого поширення шкідливої програми-бота і розширення зомбі-мережі.

Перераховані атаки на IP-мережі можливі в силу ряду причин:

- використання загальнодоступних каналів передачі даних. Найважливіші дані передаються по мережі у незашифрованому вигляді;
- вразливості в процедурах ідентифікації, реалізованих в стеку TCP/IP. Ідентифікуюча інформація на рівні IP передається у відкритому вигляді;
- відсутність в базовій версії стека протоколів TCP/IP механізмів, що забезпечують конфіденційність і цілісність переданих повідомлень;
- автентифікація відправника здійснюється за його IP-адресою. Процедура автентифікації виконується тільки на стадії встановлення з’єднання, а в подальшому достовірність прийнятих пакетів не перевіряється;
- відсутність можливості контролю за маршрутом проходження повідомлень у мережі Інтернет, що робить віддалені мережні атаки практично безкарними.

Механізми захисту від атак

Багатошаровий захист – це стратегія безпеки, в якій кілька захисних шарів розміщені через всю інформаційну систему. Це допомагає уникнути прямих атак проти інформаційної системи і даних, оскільки злом одного шару призводить зловмисника тільки до наступного рівня.

Управління інцидентами – це набір певних процесів для ідентифікації, аналізу, присвоювання пріоритетів і рішення інцидентів безпеки для відновлення нормальних сервісних операцій так швидко, як це можливо і уникнення майбутнього повторення інциденту.

Політика безпеки – це документ або набір документів, який описує управління безпекою, яке буде реалізовано в організації. Процес дослідження вразливостей і помилок проектування, який відкриває операційну систему і її застосування для атаки або зловживання.

Тестування на проникнення – це метод оцінки інформаційної безпеки системи або мережі симуляцією атаки для пошуку вразливостей, які може використовувати зловмисник. Тестування включає активний аналіз конфігурації системи, пошук недоліків проектування, архітектури мережі, технічних недоліків і вразливостей.

Підсумок

Важливо враховувати, що захист медичної інформації має відповідати вимогам стандартів безпеки в сфері охорони здоров'я та дотримуватися регуляторних вимог.

1. **Аутентифікація:**
   - *Ідентифікація особи:* Визначення ідентичності особи, яка намагається отримати доступ до медичної інформації. Це може включати в себе введення пароля, використання біометричних даних (відбиток пальця, розпізнавання обличчя) або використання смарт-карт або мобільних пристроїв для аутентифікації.
   - *Багатофакторна аутентифікація (MFA):* Використання двох чи більше методів аутентифікації для забезпечення вищого рівня безпеки. Наприклад, введення пароля, плюс введення одноразового коду, який надсилається на мобільний пристрій користувача.
   - *Цифрові сертифікати:* Використання цифрових сертифікатів для забезпечення безпеки віртуальних ідентифікаторів.
2. **Авторизація:**
   - *Керування доступом:* Після того, як особа була аутентифікована, авторизація визначає, які конкретні ресурси та функції вона може використовувати. Це включає в себе призначення ролей, прав та обмежень доступу.
   - *Ролева модель:* Системи телемедицини часто використовують ролеві моделі для призначення прав доступу на основі ролей користувачів. Наприклад, лікар може мати більше прав доступу, ніж пацієнт.
   - *Контроль доступу:* Застосування технологій контролю доступу для обмеження прав доступу користувачів до конфіденційної інформації. Це

може включати в себе використання брандмауерів, VPN, облікових записів та інших методів.

3. **Шифрування:**
   - *Захист даних в руху та спокої:* Використання шифрування для захисту передачі та зберігання медичних даних. Це допомагає уникнути незаконного доступу та забезпечує конфіденційність інформації.
4. **Моніторинг та аудит:**
   - *Журналювання подій:* Ведення журналів подій для моніторингу та аналізу дій користувачів, що має важливе значення для виявлення несанкціонованого доступу та інших безпекових інцидентів.
5. **Навчання персоналу:**
   - *Безпека поведінки користувачів:* Навчання персоналу та користувачів щодо правил безпеки та коректного використання технологій телемедицини.
6. **Захист паролів:**
   - Вимагання складних та унікальних паролів, а також регулярна їх зміна. Використання двофакторної аутентифікації для додаткового рівня захисту.
7. **Безпека мережі:**
   - Використання брандмауерів та інших засобів захисту для контролю трафіку в мережі. Захист від атак типу "человік посередника" (Man-in-the-Middle).
8. **Оновлення та патчі:**
   - Регулярне оновлення програмного забезпечення та встановлення патчів для виправлення вразливостей.
9. **Фізична безпека:**
   - Захист фізичного доступу до інформаційних ресурсів, такий як серверні приміщення, центри обробки даних та комп'ютери.
10. **Інформаційна освіта:**
    - Навчання персоналу правилам та процедурам захисту інформації, виявленню соціально інженерних атак та інших загроз безпеці.
    -

Забезпечення безпеки в телемедицині вимагає комплексного підходу та використання сучасних методів та технологій для захисту конфіденційності медичної інформації та попередження несанкціонованого доступу.

Ось деякі методи авторизації, які часто використовуються в телемедицині:

1. **Багатофакторна аутентифікація (MFA):**
   - Використання двох або більше методів для підтвердження ідентичності користувача. Наприклад, пароль може поєднуватися з одноразовим кодом, який надсилається на мобільний телефон пацієнта або лікаря.
2. **Біометрична ідентифікація:**
   - Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя чи ірису очей, для ідентифікації користувача. Це

може забезпечити високий рівень безпеки та відсікання від несанкціонованого доступу.

3. **RFID-карти та інші технології доступу:**
   - Використання безконтактних карт або інших пристроїв, які можуть бути використані для фізичного або логічного доступу до систем телемедицини.
4. **Одноразові паролі:**
   - Використання паролів, які діють лише один раз і створюються для кожного сеансу взаємодії. Це може бути важливо в тих випадках, коли безпека є особливо важливою, наприклад, при обміні чутливою медичною інформацією.
5. **Шифрування даних:**
   - Застосування шифрування для захисту транспортування та зберігання медичної інформації, що передається в мережі чи зберігається на пристроях. Це зменшує ризик доступу до конфіденційної інформації.
6. **Сертифікати безпеки:**
   - Використання цифрових сертифікатів для підтвердження автентичності та забезпечення безпечного обміну інформацією між пацієнтами, лікарями та іншими учасниками системи телемедицини.
7. **Методи біометричного відзначення та ідентифікації:**
   - Використання розпізнавання голосу, динаміки письма чи інших унікальних біометричних характеристик для ідентифікації користувачів.
8. **Ідентифікація через мобільні пристрої:**
   - Використання мобільних пристроїв для підтвердження ідентичності та доступу до медичної інформації, включаючи використання мобільних додатків та технологій NFC (Near Field Communication).