Розділ 17. Моделі загроз та моделі порушника

17.1. Загальні визначення й поняття моделі загроз та моделі порушника.
17.2. Загрози цілісності.
17.3. Загрози доступності.
17.4. Загрози конфіденційності.
17.5. Загрози автентичності.
17.6. Загрози через технічні канали.
17.7. Загрози через соціальну інженерію.

17.1. Загальні визначення й поняття моделі загроз та моделі порушника

Згідно **НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу**, визначені наступні поняття щодо **моделі загроз та моделі порушника**.

Основні загрози інформації

Інформація в комп'ютерних системах (КС) існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. (ДСТУ 2226-93). Далі терміни «інформація» і «дані» використовуються як синоніми.

Інформація для свого існування завжди вимагає наявності носія. Як **носій** інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є **класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.**

Інформація зберігає **конфіденційність**, якщо дотримуються встановлені правила ознайомлення з нею.

Інформація зберігає **цілісність**, якщо дотримуються встановлені правила її модифікації (видалення).

Інформація зберігає **доступність**, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є **загрозами конфіденційності, цілісності або доступності інформації**. Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата КС керованості може призвести до нездатності КС забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

Модель порушника

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються **чотири рівні цих можливосте**й. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з КС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– **третій рівень** визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– **четвертий рівень** визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації. Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Згідно **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі**, визначені наступні поняття щодо **моделі загроз та моделі порушника**.

Модель загроз

Загрози для інформації в АС

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення **моделі загроз** необхідно скласти **перелік суттєвих загроз**, описати **методи** і **способи** їхнього **здійснення**.

Необхідно визначити, якими з можливих **способів** можуть здійснюватися загрози в АС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Мають бути визначені **основні види загроз** для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів АС;

– наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) АС під час експлуатації;

– навмисні дії (спроби) потенційних порушників. 4.2.3 Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб’єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

– інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

– інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. **Для кожної з загроз необхідно визначити**:

– на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);

– джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

– можливі способи здійснення загроз.

Модель порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для АС;

– категорії осіб, з числа яких може бути порушник.;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей.

Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– **перший рівень** визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– **третій рівень** визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– **четвертий рівень** визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

– володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

– без одержання доступу на контрольовану територію організації (АС);

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

– з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Далі більш детально розглянемо питання моделі загроз та моделі порушника. Наявна постійна еволюція як інформаційних технологій, так і сфери захисту інформації, а також самих атакуючих: якщо ще наприкінці 20-го століття питаннями злому комп'ютерних систем займалися, як правило, захоплені ентузіасти з академічних середовищ, які не мали на меті отримання незаконного прибутку та обман компаній та громадян, то останнім часом з кожним роком зростає кількість фінансово мотивованих зловмисників. Більше того, в сучасному кіберпросторі орудують справжні армії хакерів, які підтримують і спонсорують уряди різних країн. Вони здійснюють напади на ресурси та інфраструктуру інших держав та великих корпорацій з метою одержання

розвідувальної інформації та, найчастіше, виведення з ладу об'єктів критичної інфраструктури або навіть цілих галузей промисловості. Одночасно з цим наростає також державний регуляторний тиск: усвідомлюючи важливість захисту інформації та інформаційної інфраструктури, практично всі розвинуті держави приймають законодавчі норми, що відповідають сучасним викликам. Таким чином, сучасна інформаційна безпека знаходиться на лінії перехресного вогню наступних чинників:

– висококваліфікованих атакуючих;

– IT-потреб бізнесу та держави;

– правового регулювання.

Для перемоги в умовах передусім необхідний твердий фундамент, саме чітке розуміння основних явищ, термінів, і навіть самої концепції інформаційної безпеки.

Під **захистом інформації** в класичному розумінні мається на увазі забезпечення **цілісності, конфіденційності, доступності** інформаційних ресурсів. Крім цього, **додатковими властивостями інформації** у стані захищеності є **невідмовність, справжність, підзвітність**.

Під **загрозою безпеці** інформації розуміють потенційну причину виникнення небажаного інциденту інформаційної безпеки, який може завдати шкоди активам та порушити стан захищеності інформації; інциденту може передувати несанкціонована зміна стану активу, що називається подією інформаційної безпеки.

Моделювання загроз – це ідентифікація всіх загроз, які можуть завдати шкоди активам, та векторів атак, які можуть бути використані джерелами загроз для заподіяння шкоди.

Під **ризиком інформаційної безпеки** розуміють потенційну можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації. Як і в класичному **ризик-менеджменті**, є такі способи **обробки кіберризику**:

– ігнорувати;

– прийняти;

– уникнути;

– передати;

– мінімізувати.

Вибір саме останнього, найбільш оптимального у багатьох випадках способу обробки ризику передує розробці та впровадженню систем та засобів інформаційної безпеки. При цьому при виборі та реалізації конкретних заходів щодо забезпечення інформаційної безпеки активів слід керуватися доцільністю застосування цих заходів у контексті вирішуваного бізнес-завдання, вартості активу та величини прогнозованих збитків, а також потенційних витрат зловмисників. Відповідно до загальноприйнятого підходу,

Збитки від реалізації атаки можуть бути прямими чи непрямими. Прямий збиток – це безпосередні очевидні й легко прогнозовані втрати компанії, такі як втрати прав інтелектуальної власності, розголошення секретів виробництва, зниження вартості активів або їх часткове або повне руйнування, судові витрати

та виплата штрафів і компенсацій тощо. Непрямі збитки можуть означати якісні або непрямі втрати. Якісними втратами можуть бути призупинення або зниження ефективності діяльності компанії, втрата клієнтів, зниження якості вироблених товарів або послуг. Непрямі втрати – це недоотриманий прибуток, втрата ділової репутації, додатково понесені витрати.

Загроза безпеки інформації виникає за наявності наступних взаємопов'язаних **компонентів**:

– джерела загрози;
– уразливості активу;
– способу реалізації загрози;
– об'єкта впливу;
– шкідливого впливу.

Наведемо приклад: хакер (джерело загрози) атакує непропатчений веб-сервер компанії (уразливість активу) шляхом впровадження SQL-ін'єкції (спосіб реалізації загрози) в обслуговуючу цей веб-сервер СУБД (об'єкт впливу) і незаконно отримує конфіденційну інформацію (шкідливий вплив).

Далі ці компоненти загрози інформаційній безпеці будуть розглянуті докладніше.

1. Джерелом загрози можуть бути зовнішні або внутрішні (по відношенню до об'єкта захисту, що розглядається) порушники, треті особи, сили природи.

Зовнішні порушники не є співробітниками компанії, легітимними користувачами внутрішніх інформаційних систем, аутсорсерами, підрядниками, постачальниками, замовниками та іншими особами, пов'язаними юридичними відносинами з організацією, що розглядається. Такі порушники не мають легітимного доступу до об'єкта захисту (інформаційного активу) і класифікуються за їх навичками, можливостями та мотивацією.

Прикладами зовнішніх порушників можуть бути як проурядові хакери-експерти з державною фінансовою підтримкою або найняті конкурентами кіберзлочинці, так і хактивісти, професійні кібершахраї або навіть підлітки, озброєні широкодоступними програмами хакерів.

Заходами протидії зовнішнім порушникам є практично весь спектр «класичних» способів забезпечення інформаційної безпеки: розробка та впровадження внутрішніх регламентуючих документів, засобів захисту інформації, заходів активної протидії, реагування та розслідування кіберинцидентів тощо.

Організаціям слід проводити регулярну оцінку власної схильності до ризику атаки зовнішніх зловмисників, при якій потрібно враховувати сферу діяльності, залежність від інформаційних технологій, публічність, привабливість для атакуючих, широту охоплення потенційної атаки. Загалом, саме зовнішні порушники є непередбачуваним і безконтрольним фактором кіберризику, що вимагає реалізації найсучасніших заходів та способів захисту.

Внутрішніми порушниками можуть вважатися фізичні особи – співробітники та керівники компанії, а також юридичні особи, які мають договірні відносини з компанією. Внутрішні порушники класифікуються за

цілеспрямованістю та зловмисністю їх дій, а для здійснення цілеспрямованого несанкціонованого доступу у зловмисного інсайдера мають бути мотив, спосіб та відповідна можливість для атаки.

Постачальники послуг, обладнання або персоналу також несуть ризики інформаційної безпеки – відомі випадки, коли причинами витоків ставали постачальники IT-сервісів, виробники допоміжного обладнання та співробітники компанії-підрядника. Провайдери хмарних сервісів також потрапляють до категорії потенційних внутрішніх порушників, чому може свідчити велика кількість витоків даних із некоректно налаштованих хмарних сховищ.

Крім зовнішніх та внутрішніх порушників не варто забувати і про інші джерела загроз: ***треті особи та сили природи*** можуть вплинути на діяльність компанії.

Так, третіми особами вважатимуться органи структурі державної влади, наслідки від втручання у роботу підприємства може бути пропорційні з впливом стихійного лиха. Новини про проведення слідчих заходів можуть негативно позначитися на іміджі та репутації компанії, а винесений припис про призупинення діяльності на навіть відносно нетривалий термін може фактично означати відхід компанії з ринку. Такими ж наслідками можуть стати вилучення обладнання, опечатування серверних приміщень, арешт ключових керівників компанії. Заходами мінімізації ризиків, породжених впливом третіх осіб, мають бути як неухильне виконання всіх вимог чинного законодавства, і безперервні внутрішні compliance-перевірки. Зрештою, силами природи в контексті категоризації джерел загроз є стихійні лиха, такі як природні та техногенні катастрофи, а також соціальні катастрофи: епідемії, воєнні дії, теракти, революції, страйки та інші форс-мажори.

Для мінімізації ризиків даних пригод часто потрібні великі фінансові вкладення в системи забезпечення безперервності діяльності та відновлення працездатності, а також облік даних ризиків на початкових етапах розвитку компанії: слід ретельно вибирати місце розташування офісів з урахуванням місцевості, близькості інших установ та об'єктів інфраструктури, погодних умов, стану держави та соціуму, враховувати прогнози економічного та соціального розвитку конкретного регіону присутності. Крім мінімізації ризиків впливу стихійних лих описаними вище способами, компанії можуть вибрати ще один спосіб обробки даних ризиків – **страхування**. За продуманої та грамотно обраної схеми страхових виплат можна нівелювати збитки від впливу непереборних сил на бізнес. Однак, будь-якому керівнику та співробітнику завжди варто пам'ятати про те, що життя людини безцінне в порівнянні з навіть найприбутковішим бізнесом, тому за будь-яких обставин порятунок життів та здоров'я людей має бути першим пріоритетом.

2. Вразливість – це нестача засобів захисту інформаційної системи, який може бути використаний порушником (як зовнішнім, так і внутрішнім) для реалізації загроз інформаційній безпеці. Уразливості інформаційної системи можуть бути породжені як помилками під час створення, впровадження чи експлуатації системи, і слабкістю накладених захисних засобів і застосованих

заходів.

З логічної точки зору, не може існувати ідеально захищених та безпечних інформаційних систем, які при цьому не знаходяться в ізольованому просторі, а виконують свою бізнес-функцію, тому навіть у самій здавалося б надійній та перевіреній системі можуть виявитися вразливими.

Загальноприйнятим **способом розрахунку небезпеки вразливості у кількісному** вираженні є використання метрики **CVSS (Common Vulnerability Scoring System)** американського Національного інституту стандартів та технологій (NIST, National Institute of Standards and Technology). Дана метрика дозволяє описати основні особливості вразливості та кількісно оцінити її небезпеку (за шкалою від 0 до 10) залежно від складності експлуатації, впливу на властивості безпеки активу, наявності готового експлойту та його доступності для зловмисника, можливості усунути вразливість, рівня достовірності повідомлення про наявність вразливості, а також у прив'язці до конкретного середовища експлуатації вразливої системи.

Ідея централізовано реєструвати та класифікувати вразливості знайшла свою реалізацію у кількох офіційних реєстрах уразливостей, таких як **MITRE CVE (Common Vulnerabilities and Exposures)**, **NIST NVD (National Vulnerability Database), CERT/CC VND (Vulnerability Notes Database)**.

Реєстр CVE організації MITRE ведеться з 1999 року, і за цей час у ньому були збережені дані про більш ніж 115 тисяч вразливостей. Інформацію до цього реєстру вносять CNA (CVE Numbering Authorities) – зареєстровані організації (такі як державні CERT'и), компанії-виробники ПЗ, а також незалежні дослідники безпеки, які мають повноваження надавати виявленим уразливості ідентифікатор виду CVE-YYYY-NNNN, де YYY – Рік виявлення вразливості, а NNNN – її порядковий номер. На даний момент у списку CNA присутні 98 організацій та осіб.

Крім зазначених офіційних, існує і велика кількість альтернативних реєстрів уразливостей та експлойтів, які ведуться як розробниками ПЗ (наприклад, Microsoft, Cisco, Oracle, IBM, Red Hat, Ubuntu, VMware та інші), так і окремими організаціями та ентузіастами.

Причиною виникнення вразливості може бути помилка, допущена під час розробки або налаштування програмного забезпечення. **Американський Національний інститут стандартів та технологій класифікує 124 типи помилок у своєму переліку CWE (Common Weakness Enumeration)**. Більш того, для кожної з наведених помилок на сайті організації MITRE наведено її докладний опис з прикладами вразливого коду, вказівками щодо виявлення та усунення подібних помилок з прив'язкою до стадій розробки ПЗ, а також з посиланнями на зареєстровані вразливості CVE, які були викликані цією помилкою, і **шаблони атак CAPEC (Common Attack Pattern Enumeration and Classification)**, що пов'язують помилку і можливі атаки.

Для виявлення вразливостей можна застосовувати як автоматизовані системи (сканери вразливостей, системи управління конфігураціями та версіями), так і проводити оцінку захищеності та тести на проникнення, в результаті чого організація отримує інформацію про наявність вразливостей, що

потенційно експлуатуються. Однак потрібно пам'ятати, що кожен день з'являється в середньому кілька десятків нових вразливостей, так що епізодичним аналізом не варто обходитися, а варто вибудовувати безперервний процес управління вразливістю. У його рамках організації можуть циклічно проходити інвентаризацію, класифікацію та пріоритизацію активів, аналіз поточної захищеності, пошук уразливостей та їх обробку (усунення/мінімізація/ізоляція/прийняття) відповідно до їх критичності, подальшої перевірки та оцінки ефективності пройдених кроків.

3. Способи реалізації загроз також класифікуються. Проект **MITRE ATT&CK** є базою знань про способи реалізації загроз, розширюючи список методів до **тактик, технік та процедур (TTPs – Tactics, Techniques, Procedures)**, що застосовуються атакуючими. MITRE ATT&CK пов'язаний із класифікатором шаблонів атак MITRE CAPEC, про який ми говорили раніше. Для кожної з тактик атак наводиться перелік конкретних технік, які супроводжуються детальним технічним описом реалізації атаки, списком ПЗ, що використовується атакуючими, та ідентифікаторами конкретних кіберзлочинних угруповань, що використовують відповідно до свого «почерку» ті чи інші TTPs, за якими атаку можна атрибутувати для успішного протидії чи розслідування.

4. Об'єктами шкідливого впливу при атаці можуть бути всі активи компанії, як матеріальні, так і нематеріальні: люди, інформація, процеси розробки, виробництва та постачання, канали передачі даних, програмні та апаратні засоби та компоненти систем. При цьому слід пам'ятати, що саме люди – співробітники, керівники, аутсорсери – найчастіше найслабша ланка в системі забезпечення інформаційної безпеки компанії. Якщо технічні засоби захисту функціонують відповідно до закладених у них правил і для їх ефективної роботи достатньо зробити коректне налаштування, то для мінімізації «людського фактора» при кібератаках слід безперервно вести роз'яснювальну роботу з персоналом та проводити тренування та навчання, враховуючи психологічні та соціокультурні особливості поведінки співробітників.

5. Видами шкідливого впливу зазвичай є порушення **цілісності, конфіденційності, доступності** інформаційних ресурсів, а також атаки на **невідмовність, справжність, підзвітність** інформації.

Цікавими прикладами **порушення цілісності** можуть бути різноманітні способи маніпулювання та шахрайства з даними, такі як Data Diddling (приховане внесення некоректних змін до системи з метою збереження спотворених відомостей та отримання від цього фінансової вигоди надалі – наприклад, для маніпулювання фінансовою звітністю компанії та вартістю акцій), Salami Fraud (внесення великої кількості дуже малопомітних змін протягом тривалого часу, що в результаті призводить до значних наслідків – наприклад, списання 10 копійок з кожного банківського рахунку всіх клієнтів протягом року), «логічні бомби» (впровадження програмних закладок, що призводять до спотворення даних, що зберігаються/обробляються при настанні певних умов – наприклад,(несанкціоноване нарахування підвищених відсотків за вкладом певному співробітнику банку після його звільнення).

Порушення конфіденційності інформації загрожує не тільки очевидними наслідками в короткостроковій перспективі, наприклад, при виявленні персональних даних клієнтів у відкритому доступі, але й тим, що вкрадена інформація може несподівано «спливти» через кілька років після факту компрометації – наприклад, відомості, що ганьблять компанію або керівника бути розголошені напередодні IPO або призначення на нову посаду. Крадіжка ноу-хау компанії конкурентами може призвести не тільки до втрати конкурентних переваг і частки на ринку, але й до фактів здирництва з боку атакуючих конкурентів, що загрожують оприлюднити «сірі» способи ведення бізнесу компанією.

Атаки, внаслідок яких порушується **доступність інформації**, як правило, виявляються найлегшими для виявлення, одночасно є надзвичайно руйнівними з погляду здійснення операційної діяльності та збереження репутації. Прикладами можуть бути як гучні міжнародні епідемії WannaCry або NotPetya, так і DDoS-атаки на російські платіжні системи та банки. Організації та приватні особи також все частіше стикаються з вірусами-вимагачами, які стають небезпечнішими з року в рік і здатні призупинити функціонування цілих підприємств.

Описані вище сукупні компоненти загроз інформаційної безпеки (джерела, уразливості та способи реалізації загроз, об'єкти та види шкідливого впливу) можуть бути нейтралізовані **захисними заходами**, які традиційно поділяються на організаційні, технічні, фізичні та застосовуються до співробітників, процесів та технологій. **За метою** вживаних заходів існує поділ на наступні види заходів:

– запобіжні;
– директивні;
– превентивні;
– стримуючі;
– коригувальні;
– відновлювальні;
– розслідувальні;
– компенсуючі.

Основними міжнародними стандартами практичного забезпечення інформаційної безпеки є ISO/IEC 27001:2013 Information security management systems – Requirements («Системи управління інформаційної безпеки – Вимоги») та NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations («Міри забезпечення безпеки та конфіденційності для інформаційних систем та організацій»), які включають опис організаційних та технічних вимог для розробки цілісної системи забезпечення та управління інформаційною безпекою. Слід зазначити, що всі заходи захисту, описані в стандарті NIST SP 800-53, включають також і конкретні кроки з реалізації відповідного заходу, що робить цей документ набагато більш докладним, ніж стандарт ISO/IEC 27001:2013.

Впровадження різних технічних засобів захисту доцільно проводити тільки після проходження основних етапів побудови комплексної системи

управління інформаційною безпекою: розробки внутрішніх нормативних документів у галузі ризик-менеджменту та кібербезпеки, інвентаризації та класифікації активів, оцінки та аналізу ризиків, техніко-економічного обґрунтування впровадження конкретних типів засобів захисту. Слід також врахувати, що навіть найсучасніший і «просунутий» засіб вимагає тонкого налаштування для виконання захисних бізнес-функцій у конкретній компанії, тому для економічно ефективного використання потрібно спочатку виробити розуміння того, які саме ризики закриватиме та чи інша система кіберзахисту, а потім відповідним чином її налаштувати та безперервно підтримувати в актуальному стані.

На закінчення хотілося б ще раз відзначити, що розвиток і користь від застосування сучасних інформаційних технологій йдуть пліч-о-пліч з асоційованими з ними ризиками і погрозами. Тому впровадження інформаційних технологій, як будь-який новий проект, що несе у собі певну невідомість, слід поєднувати з аналізом та обробкою ризиків. Однак часто існує застарілий підхід, при якому питання забезпечення інформаційної безпеки розглядаються у відриві від бізнес-контексту, а також не поєднуються з управлінням ризиками. Тільки цілісне розуміння компонентів актуальних загроз інформаційній безпеці разом із застосуванням методик оцінки ризиків впровадження та експлуатації тих чи інших інформаційних систем,

17.2. Загрози цілісності

Цілісність даних (англ. *data integrity*) – підтримка та забезпечення точності та цілісності даних протягом всього життєвого циклу, що є критично важливим аспектом при проектуванні, впровадженні та експлуатації систем, які зберігають, обробляють та постачають дані. Термін має широке значення і може означати різне в залежності від контексту і розділу комп'ютерних наук (криптографія, теорія електричного зв'язку, теорія інформації, безпека).

Загрози цілісності (неправомірна зміна даних). Загрози порушення цілісності – це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками – від умисних дій персоналу до виходу з ладу обладнання.

В телекомунікації цілісність даних часто перевіряють, використовуючи ґеш-суму повідомлення, обчислену алгоритмом MAC (Message authentication code).

У криптографії та інформаційній безпеці цілісність даних (в загальному) – це дані в тому вигляді, в якому вони були створені. Приклади порушень цілісності даних:

- спроба зловмисника змінити номер аккаунта в банківській транзакції, або спроба підробки документа;
- випадкове зміна інформації при передачі або при несправної роботі жорсткого диска;

– перекручування фактів засобами масової інформації з метою маніпуляції громадською думкою.

У теорії баз даних, цілісність даних означає коректність даних та їх несуперечність. Зазвичай вона також включає цілісність зв'язків, що виключає помилки зв'язків між первинним і вторинним ключем. Приміром, коли існують дочірні записи-сироти, які не мають зв'язку з батьківськими записами. Приклади порушень цілісності даних:

– існування записів-сиріт (дочірніх записів, які не мають зв'язку з батьківськими записами);

– існування однакових первинних ключів.

Для перевірки цілісності даних в криптографії використовуються ґеш-функції, наприклад, MD5. Ґеш-функція перетворює сукупність електронних даних довільного розміру в електронні данні фіксованого розміру (число). Якщо дані зміняться, то і число, що генерується ґеш-функцією, теж зміниться.

Цілісність даних – властивість, при виконанні якого дані зберігають заздалегідь певний вид і якість.

Методи забезпечення цілісності інформації

Методи і способи реалізації вимог, викладених у визначенні терміна, докладно описуються в рамках єдиної схеми забезпечення інформаційної безпеки об'єкта (захисту інформації).

Основними методами забезпечення цілісності інформації (даних) при зберіганні в автоматизованих системах є:

– забезпечення відмовостійкості (резервування, дублювання, дзеркалювання обладнання і даних, наприклад через використання RAID-масивів);

– забезпечення безпечного відновлення (резервне копіювання і електронне архівування інформації).

Одним з дієвих методів реалізації вимог цілісності інформації при її передачі по лініям зв'язку є **криптографічний захист інформації** (шифрування, ґешування, електронний цифровий підпис).

При комплексному підході до захисту бізнесу, напрям забезпечення цілісності та доступності інформації (ресурсів бізнес-процесів) переростає в план заходів, що спрямовані на забезпечення безперервності бізнесу.

Цілісність даних в криптографії

Шифрування даних саме по собі, не гарантує, що цілісність даних не буде порушена, тому в криптографії використовуються додаткові методи для гарантування цілісності даних. Під порушенням цілісності розуміється наступне:

– інверсія бітів;

– додавання нових бітів (зокрема абсолютно нових даних) третьою стороною;

– видалення яких-небудь бітів даних;

– зміна порядку слідування біт або груп біт.

У криптографії рішення задачі цілісності інформації передбачає застосування заходів, що дозволяють виявляти не стільки випадкові викривлення інформації, так як для цієї мети цілком підходять методи теорії кодування з виявленням і виправленням помилок, скільки цілеспрямоване зміна інформації активним криптоаналітиком. Процес контролю цілісності забезпечується введенням в передану інформацію надмірності. Це досягається додаванням до повідомлення деякої перевірочної комбінації. Така комбінація обчислюється згідно з певним алгоритмом і відіграє роль індикатора, за допомогою якого перевіряється цілісність повідомлення. Саме цей момент дає можливість перевірити, чи були змінені дані третьою стороною. Ймовірність того, що дані були змінені, служить мірою імітостійкості шифру.

Додаткову надлишкову інформацію, внесену до повідомлення, називають імітовставкою. Вироблятися імітовставка може як до початку, так і одночасно з шифруванням повідомлення.

Основні загрози цілісності

У більшості випадків винуватцями загроз цілісності є штатні співробітники організацій, добре знайомі з режимом роботи і заходами захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні.

З метою порушення **цілісності** зловмисник (як правило, штатний співробітник) може:

- ввести неправильні дані;
- змінити дані;
- знищити дані.

Іноді змінюються змістовні дані, іноді – службова інформація.

Потенційно уразливі з погляду порушення цілісності не тільки дані, але і програми. Впровадження шкідливого програмного забезпечення – приклад подібного порушення.

Загрозами **динамічної цілісності** є:

- порушення атомарності транзакцій,
- переупорядковування,
- крадіжка,
- дублювання даних або внесення додаткових повідомлень (мережевих пакетів і т.п.).

Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

17.3. Загрози доступності

Доступність (англ. *Availability*) – властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного)

інтервалу часу.

Суть властивості полягає в тому, що потрібний інформаційний ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Загрози доступності (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

Основні загрози доступності

Загрози доступності класифікуються за компонентами інформаційних систем (ІС), на які спрямовані загрози:

- відмова користувачів;
- внутрішня відмова інформаційної системи;
- відмова інфраструктури, що підтримує ІС.

Стосовно **користувачів** розглядаються такі загрози:

- небажання працювати з інформаційною системою (найчастіше виявляється, коли необхідно освоювати нові можливості і в разі розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);
- неможливість працювати із системою через відсутність відповідної підготовки (недолік загальної комп'ютерної освіти, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т.п.);
- неможливість працювати із системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо).

Основними **джерелами внутрішніх відмов** є:

- порушення (випадкове або навмисне) правил експлуатації;
- вихід системи зі штатного режиму експлуатації;
- помилки при (пере)конфігурації системи;
- відмови програмного і апаратного забезпечення.

Як засіб виведення системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (звичайно – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). Для виведення систем з штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок.

При прорахунках у конфігурації системи локальна програма здатна практично монополізувати процесор та/або фізичну пам'ять, звівши швидкість виконання інших програм до нуля. Простий приклад віддаленого споживання ресурсів – атака, що одержала найменування "SYN-повінь". Вона є спробою переповнити таблицю "напіввідкритих" TCP-з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше утрудняє встановлення нових з'єднань з боку легальних користувачів, тобто сервер виглядає як недоступний. По відношенню до атаки "Papa Smurf" уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на

такі пакети “з’їдають” смугу пропускання. Програма “Teardrop” видалено “підвішує” комп’ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів.

Віддалене споживання ресурсів останнім часом спостерігається в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю прямують цілком легальні запити на з’єднання та/або обслуговування. Відзначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність украй важко.

Відмови програмного забезпечення часто провокуються впровадженням в ІС так званого **шкідливого програмного забезпечення**, дії якого спрямовані на:

- руйнування даних;
- руйнування або пошкодження апаратури (носіїв даних).

Таке пошкодження може викликатися як природними причинами так і штучними. На жаль, джерела безперебійного живлення, що знаходяться в масовому використанні, не захищають від потужних короткочасних імпульсів (наприклад, блискавок), і випадки вигорання устаткування – не рідкість. Потужній короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати і штучним чином – за допомогою так званих високоенергетичних радіочастотних гармат. Однак, в наших умовах подібну загрозу слід все ж таки визнати надуманою.

Стосовно **інфраструктури** рекомендується розглядати такі загрози:

- порушення роботи (випадкове або навмисне) систем зв’язку, електроживлення, водо– і/або теплопостачання, кондиціонування;
- руйнування або пошкодження приміщень;
- неможливість або небажання обслуговуючого персоналу і/або користувачів виконувати свої обов’язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк тощо).

17.4. Загрози конфіденційності.

Конфіденційність (англ. *confidentiality*) – властивість, яка не підлягає розголосові; довірливість, секретність, суто приватність.

Конфіденційність адміністративна [mandatory confidentiality] – послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

Конфіденційність довірча [discretionary confidentiality] – послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

Конфіденційність інформації [information confidentiality] – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Загрози конфіденційності (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця), відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) та ін).

Основні загрози конфіденційності

У загальному випадку, конфіденційну інформацію можна поділити на **службову** та **предметну**.

Службова інформація (наприклад, паролі користувачів) не належить певній предметній галузі, в ІС вона грає технічну роль, але її розкриття особливо небезпечно, оскільки воно може забезпечити несанкціонований доступ до всієї інформації, зокрема предметної.

Навіть якщо інформація зберігається в комп’ютері або призначена для комп’ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться бути користувачами не одного, а кількох інформаційних сервісів. Якщо для доступу до таких систем використовуються **багаторазові паролі** або інша конфіденційна інформація, то напевно ці дані зберігатимуться не тільки в голові, але і в записнику або на папері, які користувач часто залишає на робочому столі, а то і просто губить. І справа тут не в неорганізованості людей, а в початковій непридатності парольної схеми. Неможливо пам’ятати багато різних паролів. Рекомендації щодо їх регулярної зміни тільки погіршують стан, змушуючи застосовувати нескладні схеми чергування, або взагалі прагнути звести справу до паролів, що легко запам’ятовуються і вгадуються.

Описаний клас вразливих місць можна назвати **розміщенням конфіденційних даних у середовищі, де їм не забезпечено (часто – і не може бути забезпечено) необхідний захист**. Загроза ж полягає в тому, що хтось не відмовиться дізнатися секрети, які самі просяться в руки. Крім паролів, що зберігаються в записниках користувачів, до цього класу потрапляє передача конфіденційних даних у відкритому вигляді (у розмові, в листі, мережею), яка робить можливим перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі і т.п.), але ідея одна – здійснити доступ до даних у той

час, коли вони найменше захищені.

Вельми небезпечною загрозою є **виставки**, на які багато організацій відправляють устаткування з виробничої мережі, з усіма збереженими на них даними, залишаючи тим самим паролі. При віддаленому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть в межах захищеної мережі організації, а в об'єднаній мережі виставки – це дуже суворе випробування чесності всіх учасників.

Ще один приклад загрози, про яку часто забувають, – зберігання даних **на резервних носіях**. Для захисту даних на основних носіях застосовуються розвинені системи управління доступом, тоді як копії нерідко просто лежать у шафах і дістати доступ до них може багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються багатьма каналами, їх захист може виявитися достатньо складним і дорогим. Технічні засоби перехоплення доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може хто завгодно, тому цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, а й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але і для комп'ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто гублять.

Небезпечною нетехнічною загрозою конфіденційності є методи **соціальної інженерії**, такі як **маскарад** – виконання дій під виглядом особи, що володіє повноваженнями для доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести **зловживання повноваженнями**. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, дістати доступ до пошти будь-якого користувача і т.д.

Інший приклад – нанесення збитку при сервісному обслуговуванні. Звичайно сервісний інженер дістає необмежений доступ до устаткування і має можливість діяти в обхід програмних захисних механізмів.

Такі основні загрози, які завдають найбільшого збитку суб'єктам інформаційних відносин.

17.5. Загрози автентичності

Автентифіка́ція – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Існують наступні визначення автентичності згідно стандартів NIST:

– Властивість того, що дані походять із передбачуваного джерела, згідно NIST SP 800-38 та NIST SP 800-63-3.

– Властивість бути справжнім, бути перевіреним і довіряти; впевненість у дійсності передачі, повідомлення або автора повідомлення, згідно NIST SP 800-30, NIST SP 800-37, NIST SP 800-39, NIST SP 800-53, NIST SP 800-60,

NIST SP 800-137.

5 поширених типів автентифікації

Кіберзлочинці завжди вдосконалюють свої атаки. У результаті групи безпеки стикаються з багатьма проблемами, пов'язаними з автентифікацією. Ось чому компанії починають впроваджувати більш складні стратегії реагування на інциденти, включаючи автентифікацію як частину процесу. У наведеному нижче списку розглядаються деякі поширені методи автентифікації, які використовуються для захисту сучасних систем.

1. Автентифікація на основі пароля

Паролі є найпоширенішими методами автентифікації. Паролі можуть бути у вигляді рядка літер, цифр або спеціальних символів. Щоб захистити себе, вам потрібно створити надійні паролі, які містять комбінацію всіх можливих варіантів.

Однак паролі схильні до фішингових атак і поганої гігієни, що послаблює ефективність. Середня людина має близько 25 різних облікових записів в Інтернеті, але лише 54% користувачів використовують різні паролі для своїх облікових записів.

Правда полягає в тому, що паролів потрібно запам'ятати багато. У результаті багато людей обирають зручність, а не безпеку. Більшість людей використовують прості паролі замість створення надійних, оскільки їх легше запам'ятати.

Суть полягає в тому, що паролі мають багато недоліків і недостатні для захисту інформації в Інтернеті. Хакери можуть легко вгадати облікові дані користувача, переглядаючи всі можливі комбінації, поки не знайдуть збіг.

2. Багатофакторна автентифікація

Багатофакторна автентифікація (MFA) – це метод автентифікації, який вимагає двох або більше незалежних способів ідентифікації користувача. Приклади включають коди, згенеровані зі смартфона користувача, тести Captcha, відбитки пальців, голосові біометричні дані або розпізнавання обличчя.

Методи та технології автентифікації MFA підвищують довіру користувачів, додаючи кілька рівнів безпеки. MFA може бути гарним захистом від більшості зломів облікових записів, але він має свої підводні камені. Люди можуть втратити свої телефони або SIM-карти і не зможуть згенерувати код автентифікації.

3. Автентифікація на основі сертифіката

Технології автентифікації на основі сертифікатів ідентифікують користувачів, машини чи пристрої за допомогою цифрових сертифікатів. Цифровий сертифікат – це електронний документ, створений за ідеєю водійського посвідчення чи паспорта.

Сертифікат містить цифрову ідентифікацію користувача, включаючи відкритий ключ, і цифровий підпис центру сертифікації. Цифрові сертифікати підтверджують право власності на відкритий ключ і видаються тільки центром сертифікації. Користувачі надають свої цифрові сертифікати під час входу на сервер. Сервер перевіряє достовірність цифрового підпису та центру сертифікації. Потім сервер використовує криптографію, щоб підтвердити, що

користувач має правильний закритий ключ, пов'язаний із сертифікатом.

4. Біометрична автентифікація

Біометрична автентифікація – це процес безпеки, який базується на унікальних біологічних характеристиках людини. Ось основні переваги використання технологій біометричної автентифікації:

– Біологічні характеристики можна легко порівняти з авторизованими характеристиками, збереженими в базі даних.

– Біометрична автентифікація може контролювати фізичний доступ, якщо вона встановлена на воротах і дверях.

– Ви можете додати біометричні дані в процес багатофакторної автентифікації.

Технології біометричної автентифікації використовуються споживачами, урядами та приватними корпораціями, включаючи аеропорти, військові бази та національні кордони. Ця технологія набуває все більшого поширення завдяки можливості досягти високого рівня безпеки, не створюючи тертя для користувача. Загальні методи біометричної автентифікації включають:

– **Розпізнавання обличчя** – зіставляє різні характеристики обличчя особи, яка намагається отримати доступ до затвердженого обличчя, яке зберігається в базі даних. Розпізнавання облич може бути непослідовним під час порівняння облич під різними кутами або порівняння людей, які виглядають схожими, наприклад, близьких родичів. Жвавість обличчя, як пасивна жвавість, запобігає підробці.

– **Сканери відбитків пальців** – зіставте унікальні візерунки на відбитках пальців людини. Деякі нові версії сканерів відбитків пальців можуть навіть оцінювати судинні малюнки на пальцях людей. Сканери відбитків пальців наразі є найпопулярнішою біометричною технологією для повсякденних споживачів, незважаючи на їх часті неточності. Таку популярність можна віднести до iPhone.

– **Розпізнавання мовця** – також відоме як біометрія голосу, вивчає шаблони мовлення мовця для формування певних форм і звукових якостей. Пристрій із захистом голосу зазвичай покладається на стандартні слова для ідентифікації користувачів, як і пароль.

– **Сканери очей** – включають такі технології, як розпізнавання райдужної оболонки ока та сканери сітківки ока. Сканери райдужної оболонки проектують яскраве світло в око та шукають унікальні візерунки в кольоровому кільці навколо зіниці ока. Потім шаблони порівнюються із затвердженою інформацією, що зберігається в базі даних. Автентифікація на основі ока може мати неточності, якщо людина носить окуляри або контактні лінзи.

5. Автентифікація на основі маркерів

Технології автентифікації на основі токенів дозволяють користувачам вводити свої облікові дані один раз і отримувати натомість унікальний зашифрований рядок випадкових символів. Потім ви можете використовувати маркер для доступу до захищених систем замість того, щоб знову вводити свої облікові дані. Цифровий маркер підтверджує, що ви вже маєте дозвіл на доступ. Варіанти використання автентифікації на основі маркерів включають RESTful API, які використовуються кількома фреймворками та клієнтами.

Атаки на автентифікацію

На даний час виявлені наступні атаки на автентифікацію:

1. Клонування або запозичення «Shoulder Surfing».
2. Sniff the credentials (шукати облікові дані).
3. Метод проб і помилок.
4. Атака на відмову в обслуговуванні (DoS, DDoS).
5. Отримати з резервної копії.
6. Атаки на автентифікацію користувача веб-сайту.
7. Атаки на паролі (Фішинг; Атака «людина посередині; Атака грубою силою; Додавання облікових даних; Кейлоггери).
8. Слабкі облікові дані для входу.
9. Перерахування імен користувачів.
10. Базова автентифікація HTTP.
11. Погане керування сеансами.
12. Залишення в системі.
13. SQL ін'єкція.
14. Небезпечна зміна та відновлення пароля.
15. Помилка двофакторної автентифікації.
16. Вразлива логіка автентифікації
17. Людська недбалість

Розглянемо їх більш детально:

1. Клонування або запозичення «Shoulder Surfing» – це атака, яка зазвичай виконується шляхом перегляду через плече або пошуку облікових даних для входу та використання їх для входу.

2. Sniff the credentials (шукати облікові дані) – це метод, який фіксує облікові дані під час їх передачі в процес входу. Збираємо пакети через wireshark або подібне програмне забезпечення для аналізу пакетів і шукаємо паролі та токени.

3. Метод проб і помилок – ця атака просто пробує різні комбінації, поки зловмисник не отримає одне право, щоб мати можливість увійти.

4. Атака на відмову в обслуговуванні (DoS, DDoS) – полягає в тому, що зловмисник може пошкодити систему, що заблокує оцінку системи іншими, тобто перевантаження системи для блокування користувача, запобігання доступу до системи.

5. Отримати з резервної копії – це можливість отримати інформацію про вхід із резервної копії на жорсткому диску та використовувати інформацію для входу, щоб отримати доступ до облікового запису.

6. Атаки на автентифікацію користувача веб-сайту.

Цей тип атаки спрямований і намагається використати процес автентифікації, який веб-сайт використовує для перевірки ідентичності користувача, служби чи програми.

Таблиця 13.1 – Атаки автентифікації користувача веб-сайту

Типи атак	Опис атаки
Груба сила	Дозволяє зловмиснику вгадати ім’я користувача, пароль, номер кредитної картки або криптографічний ключ за допомогою автоматизованого процесу проб і помилок.
Недостатня автентифікація	Дозволяє зловмиснику отримати доступ до веб-сайту, що містить конфіденційний вміст або функції, без належної автентифікації на веб-сайті.
Слабка перевірка відновлення пароля	Дозволяє зловмиснику отримати доступ до веб-сайту, який надає йому можливість незаконно отримати, змінити або відновити пароль іншого користувача.

Сигнатури, викликані цією атакою

Таблиця 13.2 – Сигнатури, викликані атаками автентифікації, включають:

Ім'я підпису	Опис
HTTP_Auth_ContainsBinary	Шукає автентифікацію HTTP, яка містить двійкові дані.
HTTP_Auth_TooLong	Виявляє рядок авторизації HTTP, який довший за настроюване системою значення максимальної довжини авторизації HTTP. Цей підпис замінює HTTP_NS_Admin_Overflow.
HTTP_Authentication	Виявляє базову автентифікацію HTTP на веб-сервері та реєструє імена користувачів і паролі. Ця подія безпеки класифікується як подія аудиту. Це не обов’язково вказує на атаку чи загрозу у вашій мережі.
HTTP_Authentication_Format_String	Виявляє атаку на рядок формату базової автентифікації HTTP в іменах користувачів і паролях.
HTTP_IIS_Hit_Highlighting_Auth_ Bypass	Шукає спроби обійти обмеження безпеки за допомогою вразливості у функціях підсвічування звернень сервера Microsoft IIS.
HTTP_Login_Known_User	Визначає ім’я для входу та зіставляє його з визначеними користувачем іменами для входу для добре відомих імен для входу.
HTTPS_ClearText_Session	Виявляє дійсний запит HTTP та відповідь на порт 443, який не зашифровано.

7. Атаки на паролі

Атаки на паролі є однією з найпоширеніших форм зламу корпоративних і особистих даних. Атака на пароль – це просто спроба хакера викрасти ваш пароль. 81% витоків даних було спричинено скомпрометованими обліковими даними. Оскільки паролі можуть містити невелику кількість літер і цифр, паролі стають менш безпечними. Хакери знають, що багато паролів розроблено погано, тому атаки на паролі залишатимуться методом атаки, доки паролі використовуються.

Захистіть себе від атак на пароль за допомогою наведеної нижче інформації.

7.1. Фішинг

Фішинг – це коли хакер, видаючи себе за надійну сторону, надсилає вам шахрайський електронний лист, сподіваючись, що ви добровільно розкриєте свою особисту інформацію. Іноді вони призводять вас до підроблених екранів «скинути пароль»; в інших випадках посилання встановлюють шкідливий код на ваш пристрій. Ми висвітлюємо кілька прикладів у блозі OneLogin.

Ось кілька прикладів фішингу:

– Ви отримуєте електронний лист від щось схоже на goodwebsite.com із проханням скинути пароль, але ви не читали уважно, а насправді це goodwobsite.com. Ви «скидаєте свій пароль», і хакер викрадає ваші облікові дані.

– Хакер націлює вас саме на електронну пошту, яка нібито надійшла від друга, колеги чи партнера. Він має коротку загальну анонсу («Перегляньте рахунок-фактуру, який я долучив, і дайте мені знати, чи це має сенс») і сподівається, що ви клацнете зловмисне вкладення.

– Ви отримуєте текстове повідомлення (SMS-фішинг або смішинг) або телефонний дзвінок (голосовий фішинг або вішинг) від хакера, який повідомляє вам, що ваш обліковий запис заморожено або що виявлено шахрайство. Ви вводите дані свого облікового запису, і хакер їх краде.

– Ви або ваша організація отримуєте електронний лист нібито від високопоставленої особи у вашій компанії. Ви не виконуєте домашнє завдання щодо правдивості електронної пошти та не надсилаєте конфіденційну інформацію хакеру.

Щоб уникнути фішингових атак, виконайте такі дії:

– **Перевірте, хто надіслав електронний лист**: подивіться на рядок «Від:» у кожному електронному листі, щоб переконатися, що особа, за яку себе видають, відповідає адресі електронної пошти, яку ви очікуєте.

– **Ще раз перевірте джерело**: якщо ви сумніваєтеся, зв’яжіться з особою, від якої надійшов електронний лист, і переконайтеся, що він був відправником.

– **Зверніться до своєї IT-команди**: IT-відділ вашої організації часто може сказати вам, чи електронний лист, який ви отримали, є законним.

7.2. Атака «людина посередині».

Атаки типу «людина посередині» (MitM) – це випадки, коли хакер або скомпрометована система сидить між двома нескомпрометованими людьми чи системами та розшифровує інформацію, яку вони передають один одному,

зокрема паролі. Якщо Аліса та Боб передають нотатки в класі, але Джеремі має передати ці нотатки, Джеремі має можливість бути людиною посередині. Подібним чином у 2017 році Equifax видалив свої програми з App Store і Google Play, оскільки вони передавали конфіденційні дані через незахищені канали, де хакери могли викрасти інформацію про клієнтів.

Щоб запобігти атакам типу "людина посередині":

– **Увімкніть шифрування на маршрутизаторі.** Якщо до вашого модему та маршрутизатора може отримати доступ будь-хто з вулиці, він може використовувати технологію «аналізатора», щоб побачити інформацію, яка передається через нього.

– **Використовуйте надійні облікові дані та двофакторну автентифікацію.** Багато облікових даних маршрутизатора ніколи не змінюються з імені користувача та пароля за замовчуванням. Якщо хакер отримує доступ до адміністрування вашого маршрутизатора, він може перенаправити весь ваш трафік на свої зламані сервери.

– **Використовуйте VPN.** Захищена віртуальна приватна мережа (VPN) допоможе запобігти атакам типу "людина посередині", гарантуючи, що всі сервери, на які ви надсилаєте дані, є надійними.

7.3. Атака грубою силою

Якщо пароль еквівалентний використанню ключа, щоб відкрити двері, атака грубою силою – це використання тарану. Хакер може спробувати 2,18 трильйона комбінацій пароля/імена користувача за 22 секунди, і якщо ваш пароль простий, ваш обліковий запис може опинитися під прицілом.

Атака грубої сили, наприклад атака за словником, – це спроба отримати незаконний доступ до системи або облікового запису користувача шляхом введення великої кількості випадково згенерованих або попередньо згенерованих комбінацій імен користувачів і паролів, доки не буде знайдено те, що працює.

Якщо є помилкова система захисту від грубої сили, наприклад помилка в логіці автентифікації, брандмауері або протоколі захищеної оболонки (SSH), зловмисники можуть викрасти облікові дані та процеси для входу, ставлячи під загрозу безпеку облікових даних користувача.

Щоб запобігти атакам грубої сили:

– Використовуйте складний пароль. Різниця між шестизначним паролем, що складається лише з малих літер, і десятизначним паролем із змішаним регістром, із змішаними символами, величезна. Зі збільшенням складності вашого пароля ймовірність успішної атаки грубою силою зменшується.

– Увімкніть і налаштуйте віддалений доступ. Запитайте у відділі IT, чи використовує ваша компанія керування віддаленим доступом. Такий інструмент керування доступом, як OneLogin, зменшить ризик атаки методом грубої сили.

– Потрібна багатофакторна автентифікація. Якщо у вашому обліковому записі ввімкнено багатофакторну автентифікацію (MFA), потенційний хакер може надіслати запит на доступ до вашого облікового запису лише другому фактору. Імовірно, хакери не матимуть доступу до вашого мобільного пристрою чи відбитка пальця, а це означає, що вони будуть заблоковані у вашому

обліковому записі.

7.4. Атака за словником

Тип атаки грубої сили, атаки за словником покладаються на нашу звичку вибирати «основні» слова як наш пароль, найпоширеніші з яких хакери зібрали в «злом словників». Більш складні словникові атаки включають слова, важливі для вас особисто, як-от місце народження, ім'я дитини чи ім'я домашньої тварини.

Щоб запобігти атаці за словником:

– Ніколи не використовуйте слова зі словника як пароль. Якщо ви прочитали це в книзі, воно ніколи не повинно бути частиною вашого пароля. Якщо вам потрібно використовувати пароль замість інструменту керування доступом, розгляньте можливість використання системи керування паролями.

– Блокування облікових записів після багатьох невдалих паролів. Блокування облікового запису може викликати розчарування, коли ви на короткий час забули пароль, але альтернативою часто є незахищеність облікового запису. Зробіть п'ять або менше спроб, перш ніж ваша програма повідомить вам заспокоїтися.

– Розгляньте можливість інвестування в менеджер паролів. Менеджери паролів автоматично генерують складні паролі, які допомагають запобігти словниковим атакам.

7.5. Додавання облікових даних

Якщо вас раніше зламували, ви знаєте, що ваші старі паролі, ймовірно, просочилися на поганий веб-сайт. Додавання облікових даних використовує облікові записи, паролі яких ніколи не змінювалися після злому. Хакери спробують різні комбінації колишніх імен користувачів і паролів, сподіваючись, що жертва ніколи їх не змінила.

Щоб запобігти надходженню облікових даних:

– Контролюйте свої облікові записи. Існують платні служби, які відстежуватимуть ваші ідентифікаційні дані в Інтернеті, але ви також можете скористатися безкоштовними службами, як-от haveIbeenpwned.com, щоб перевірити, чи пов'язана ваша адреса електронної пошти з нещодавніми витоками.

– Регулярно змінюйте свої паролі. Чим довше один пароль залишається незмінним, тим більша ймовірність того, що хакер знайде спосіб його зламати.

– Використовуйте менеджер паролів. Подібно до атаки за словником, багатьох атак із підкиданням облікових даних можна уникнути, маючи надійний і безпечний пароль. Менеджер паролів допомагає підтримувати їх.

7.6. Кейлоггери

Клавіатурні шпигуни – це тип шкідливого програмного забезпечення, призначеного для відстеження кожного натискання клавіш і звітування про це хакеру. Як правило, користувач завантажує програмне забезпечення, вважаючи його законним, лише для того, щоб установити кейлоггер без попередження.

Щоб захистити себе від кейлоггерів:

– Перевірте своє фізичне обладнання. Якщо хтось має доступ до вашої робочої станції, він може встановити апаратний кейлоггер для збору інформації

про натискання клавіш. Регулярно перевіряйте свій комп'ютер і територію навколо, щоб переконатися, що знаєте кожну частину апаратного забезпечення.

– Запустіть перевірку на віруси. Використовуйте перевірене антивірусне програмне забезпечення для регулярного сканування комп'ютера. Антивірусні компанії зберігають свої записи про найпоширеніші кейлоггери шкідливих програм і позначають їх як небезпечні.

Запобігання атакам на пароль

Найкращий спосіб усунути атаку на пароль – це уникати її. Запитайте свого IT-фахівця про проактивне інвестування в загальну політику безпеки, яка включає:

– **Багатофакторна автентифікація.** Використання фізичного токена (наприклад, Yubikey) або персонального пристрою (наприклад, мобільного телефону) для автентифікації користувачів гарантує, що паролі не є єдиними воротами для доступу.

– **Віддалений доступ.** Використання розумної платформи віддаленого доступу, як-от OneLogin, означає, що окремі веб-сайти більше не є джерелом довіри користувачів. Натомість OneLogin гарантує, що особу користувача підтверджено, а потім здійснює вхід.

– **Біометрія.** Зловмиснику буде дуже важко відтворити ваш відбиток пальця чи форму обличчя. Увімкнення біометричної автентифікації перетворює ваш пароль лише на одну з кількох точок довіри, які хакер повинен подолати.

8. Слабкі облікові дані для входу

Коли користувачі реєструються для облікового запису на сайті або в програмі, яка використовує вхід на основі пароля, їм пропонується створити ім'я користувача та пароль.

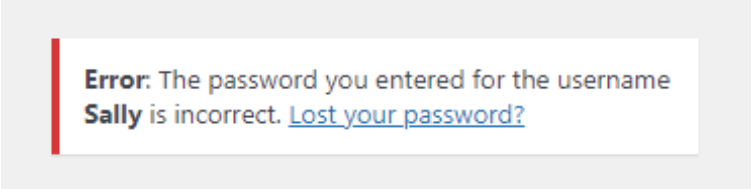
Однак якщо пароль передбачуваний, це може призвести до вразливості в процесі автентифікації. Передбачувані імена користувачів можуть полегшити зловмисникам націлювання на конкретних користувачів.

Замість того, щоб використовувати повну атаку грубої сили, зловмисники шукатимуть облікові записи з паролями, які легко вгадати, які використовуються занадто часто.. Вони спробують ввести такі звичайні облікові дані, як «admin», «admin1» і «password1». Без обмежень на слабкі паролі навіть сайти, захищені від атак грубої сили, можуть виявитися скомпрометованими.

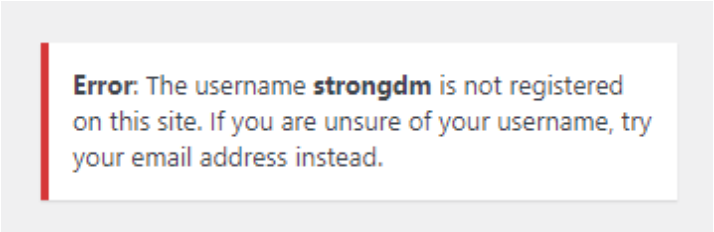
9. Перерахування імен користувачів

Перерахування імен користувачів не є точною вразливістю автентифікації. Але це може полегшити життя зловмисника, знизивши вартість інших атак, таких як атаки грубої сили або слабкі перевірки облікових даних.

Цей процес нумерації імені користувача підтверджує, чи дійсне ім'я користувача. Наприклад:



У цьому випадку ім'я користувача правильне, а пароль – ні.



Тут ім’я користувача недійсне.

Проблема з нумерацією імен користувачів полягає в тому, що зловмисники можуть визначити, які імена користувачів дійсні. Потім вони можуть спробувати зламати дійсні облікові записи користувачів за допомогою методів грубої сили, не витрачаючи час і гроші на тестування безлічі недійсних імен облікових записів.

10. Базова автентифікація HTTP

Цей класичний протокол веб-автентифікації простий у застосуванні, однак він не позбавлений ризиків.

Базова автентифікація HTTP проста: під час кожного запиту надсилаються ім’я користувача та пароль. Однак якщо відповідні протоколи безпеки, такі як шифрування сеансу TLS, не використовуються для зв’язку, інформація про ім’я користувача та пароль може бути надіслана відкрито, що полегшить зловмисникам викрадення облікових даних.

Оскільки включені облікові дані містять дуже мало контексту, їх можна легко використати в атаках, таких як підробка міжсайтових запитів (CSRF). Крім того, оскільки вони додаються до кожного окремого запиту, сучасні браузери зазвичай кешують цю інформацію на невизначений термін, з мінімальною можливістю «вийти» та запобігти повторному використанню облікових даних локальним зловмисником у майбутньому.

11. Погане керування сеансами

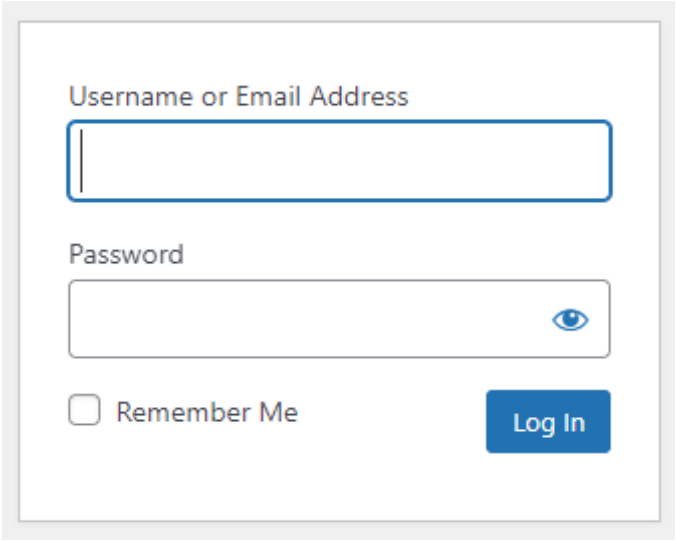
Уразливість в управлінні ідентифікаторами сеансів призводить до викрадення дійсних автентифікованих сеансів. Це одна з поширених веб-уразливостей для обходу паролів.

Існує кілька вразливостей, пов’язаних із неправильним керуванням сеансом, наприклад відсутність тайм-аутів сеансу, виявлення ідентифікаторів сеансу в URL-адресах, файли cookie сеансу без установленого прапорця «Лише Http» і погане визнання сеансу недійсним.

Якщо зловмисники можуть захопити контроль над існуючим сеансом, вони легко проникають у систему, припускаючи особу вже автентифікованого користувача, повністю минаючи процес автентифікації.

12. Залишення в системі

Прапорець «Запам’ятати мене» або «Залишати мене в системі» під формою входу дозволяє надзвичайно легко залишатися в системі після закриття сеансу. Він генерує файл cookie, який дозволяє вам пропустити процес входу.



Однак це може призвести до вразливості автентифікації на основі файлів cookie, якщо зловмисник може передбачити файл cookie або визначити шаблон його створення. Вони можуть використовувати такі зловмисні методи, як атаки грубої сили, щоб передбачити файли cookie, і міжсайтовий сценарій (XSS) для злому облікових записів користувачів, дозволяючи зловмисному серверу використовувати законний файл cookie.

Якщо файл cookie погано розроблений або захищений, зловмисники можуть отримати паролі або інші конфіденційні (і захищені законом) дані, такі як адреси користувачів або дані облікового запису, із збережених файлів cookie.

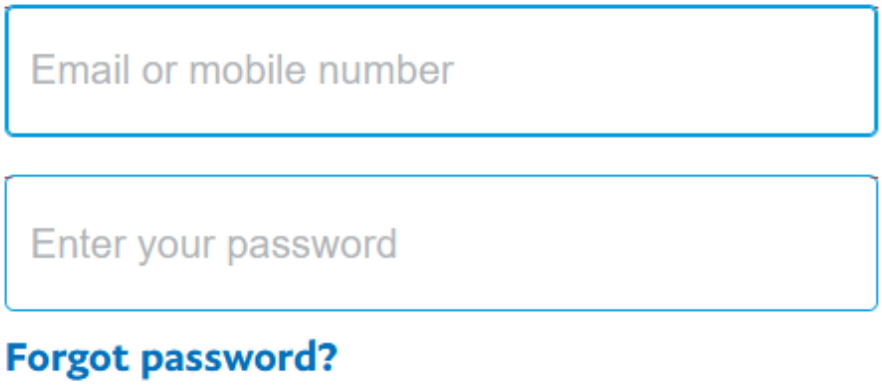
13. SQL-ін'єкція

SQL-ін’єкція – це вектор атаки, який неочікуваним чином використовує зловмисний код SQL для маніпулювання та доступу до бази даних.

Ін’єкції SQL можуть уможливити атаки на механізми автентифікації шляхом викрадення відповідних даних (наприклад, погано захищених ґешів паролів) із незахищеної бази даних. Вони також можуть обійти механізми автентифікації, якщо впроваджений код SQL виконується внутрішнім (і вже авторизованим) інструментом, який не зміг достатньо перевірити зовнішній вхід.

14. Небезпечна зміна та відновлення пароля

Іноді користувачі забувають або просто хочуть змінити свої паролі та натискають посилання «Забули пароль» або «Забули пароль».



Процес скидання пароля створює вразливість автентифікації, якщо програма використовує слабкий механізм відновлення пароля, як-от прості контрольні запитання, відсутність CAPTCHA або повідомлення електронної пошти для скидання пароля з надто довгими часами очікування або без них.

Якщо функція відновлення пароля має недоліки, зловмисники потенційно можуть використати методи грубої сили або отримати доступ до інших зламаних облікових записів, щоб отримати доступ до облікових записів користувачів і облікових даних, які добре захищені за звичайних обставин.

15. Помилка двофакторної автентифікації

Хоча двофакторна автентифікація (2FA) ефективна для безпечної автентифікації, вона може спричинити критичні проблеми безпеки, якщо її не впровадити належним чином. Зловмисники можуть визначити чотири- та шестизначні коди перевірки 2FA за допомогою атак обміну SIM-картою, якщо вони надіслані через SMS. Деяка двофакторна автентифікація також не є справді двофакторною; якщо користувач намагається отримати доступ до конфіденційної інформації на викраденому телефоні за допомогою кешованих облікових даних, «другий фактор», який надсилає повідомлення на той самий телефон, не додає додаткової безпеки. Уразливість двофакторної автентифікації також може виникнути, якщо немає захисту від грубої сили для блокування облікового запису після певної кількості спроб входу.

16. Вразлива логіка автентифікації

Логічні вразливості поширені в програмних додатках. Це відбувається в результаті поганого кодування або дизайну, що впливає на автентифікацію та авторизацію доступу та функціональність програми. Помилка логіки програми може бути спричинена зловживанням функціональністю, слабкими заходами безпеки або пропущеним кроком у процедурі перевірки.

Наприклад, програма може запропонувати користувачеві відповісти на таємне запитання, яке логіка вважає таким, що «знає лише правильна особа». Але такі запитання, як день народження користувача чи дівоче прізвище матері, часто знайти легко. Ця вразливість дозволяє кібер-зловмисникам легко обійти автентифікацію та отримати незаконний доступ до таких облікових записів.

17. Людська недбалість

Згідно зі звітом Shred-it за 2020 рік, до 31% керівників старшого рівня назвали недбалість співробітників другою основною причиною витоку їхніх даних. Людська помилка може призвести до серйозних уразливостей автентифікації, якими набагато легше скористатися, ніж атаками грубої сили, ін’єкціями SQL та обходами автентифікації. Ця недбалість включає такі дії, як:

– Залишати комп’ютер увімкненим і незаблокованим у громадському місці
– Втрата пристроїв через крадіжку.
– Витік конфіденційної інформації незнайомцям.
– Написання поганого коду.

17.6. Загрози через технічні канали

Для перехоплення, обробки та аналізу інформації за допомогою **каналів витоку інформації (КВІ)** можуть використовуватися різноманітні **технічні засоби (ТЗс)**, а також люди (порушники). Тоді існуючі КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів:

– «людина – людина»;

– «людина – ТЗс»;

– «ТЗс – ТЗс»;

– «ТЗс – людина».

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється ***узагальнений канал витоку***, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за вищезгаданими чотирма типами каналів від порушника до носія інформації, то виникає так званий ***узагальнений канал інформаційного впливу на носій інформації (канал спеціального впливу)***. Залежно від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні та інші способи і засоби. Параметрами, на які задумано здійснити вплив, можуть бути різні характеристики матеріальних носіїв, у тому числі й власні характеристики головного прямого носія інформації – людини.

Найбільший потенціал інформативності мають КВІ, у яких для отримання конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву **технічних (ТКВІ)**. Структура будь-якого ТКВІ, що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації.

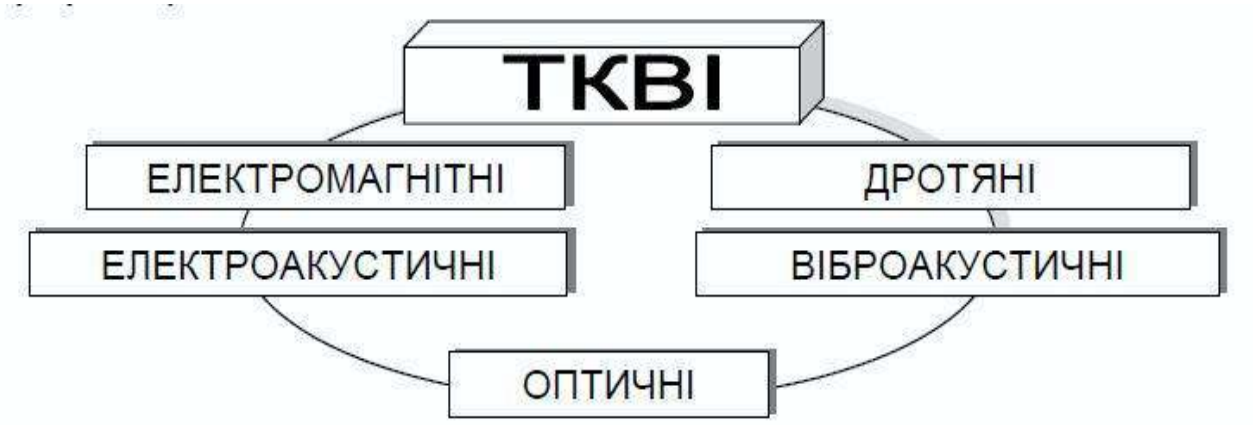


Рисунок 17.1 – Види технічних каналів витоку інформації (ТКВІ)

Структура технічних каналів витоку інформації (ТКВІ)

При цьому процес передачі повідомлень розбивається на три основні етапи.

– На початку кожне повідомлення a(t) перетворюється передавачем у небезпечний (інформаційний) сигнал b(t).

– Небезпечний сигнал переміщується трактом його поширення, де на нього діє завада p(t), внаслідок чого він частково затухає.

– Далі одержаний на приймальній стороні небезпечний сигнал b'(t) перетворюється приймачем порушника в повідомлення a'(t). Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача b'(t) буде випадковим чином відрізнятися від b(t) і повідомлення a(t) може відрізнятися від a'(t).

ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і за допомогою тільки приймачів, які приймають небезпечні сигнали, утворені несанкціонованим перетворенням сигналів з каналів передачі даних у технічних засобах обробки інформації.

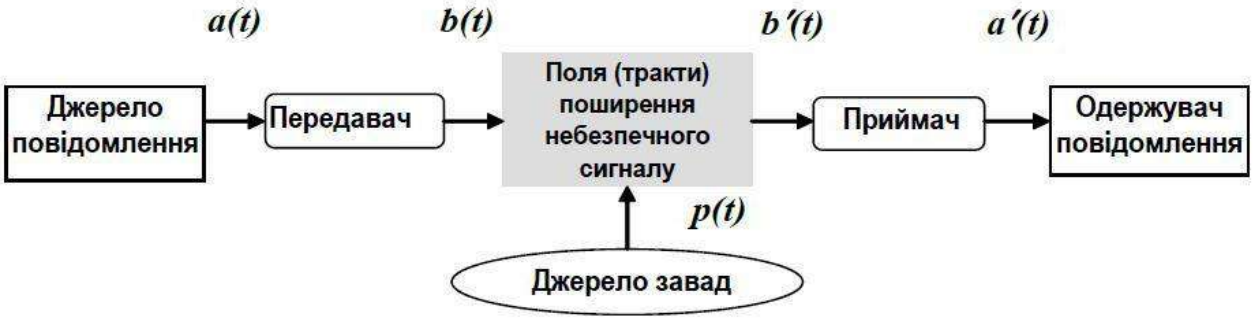


Рисунок 17.2 – Процес передачі повідомлень

Класифікація технічних каналів витоку інформації (ТКВІ)

Схема можливих каналів витоку і несанкціонованого доступу до інформації в типовому одноповерховому приміщенні показана на рисунку нижче.

Рисунок 17.3 – Можливі канали витоку інформації (КВІ) та несанкціонованого доступу (НСД)

На рисунку використанні наступні умовні позначення:
1 – Витік за рахунок структурного звуку в стінах і перекриттях.
2 – Зняття інформації із стрічки принтера, погано стертих дискет і т. п.
3 – Зняття інформації з використанням відеозакладок.
4 – Програмно-апаратні закладки в ПЕОМ.
5 – Радіозакладки у стінах і меблях.
6 – Зняття інформації із системи вентиляції.
7 – Лазерне зняття акустичної інформації з вікон.
8 – Виробничі й технологічні відходи.
9 – Комп'ютерні віруси, логічні бомби і т.п.
10 – Зняття інформації шляхом наведень і "нав'язування".
11 – Дистанційне зняття відеоінформації (оптика).

12 – Зняття акустичної інформації з використанням диктофонів.
13 – Крадіжка носіїв інформації.
14 – Високочастотний канал витоку в побутовій техніці.
15 – Зняття інформації направленим мікрофоном.
16 – Внутрішні канали витоку інформації (через обслуговуючий персонал).
17 – Несанкціоноване копіювання.
18 – Витік за рахунок побічного випромінювання терміналу.
19 – Зняття інформації за рахунок використання "телефонного вуха".
20 – Зняття з клавіатури і принтера за акустичним каналом.
21 – Зняття з монітора з електромагнітного канала.
22 – Візуальне зняття з монітора і принтера.
23 – Наведення на лінії комунікацій і сторонні провідники.
24 – Витік через лінії зв'язку.
25 – Витік ланцюгами заземлення.
26 – Витік мережею електрогодинника.
27 – Витік трансляційною мережею та гучномовним зв'язком.
28 – Витік охоронно-пожежною сигналізацією.
29 – Витік мережею електроживлення.
30 – Витік мережею опалювання, газо- і водопостачання.

Компрометація інформації (один з видів інформаційних інфекцій). Реалізується, як правило, за допомогою несанкціонованих змін у базі даних, у результаті чого її споживач змушений або відмовитися від неї, або докладати додаткових зусиль для виявлення змін і відновлення правдивих відомостей. При використанні скомпрометованої інформації споживач піддається небезпеці прийняття правильних рішень.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є наслідком її витоку й засобом її компрометації. З іншого боку, воно має самостійне значення, тому що може завдати великої шкоди керованій системі (аж до повного виходу ІТ з ладу) або її абонентам.

Помилкове використання інформаційних ресурсів, які є санкціонованими, може призвести до руйнування, витоку або компрометації зазначених ресурсів. Дана загроза найчастіше є наслідком помилок, наявних у ПЗ ІТ.

Несанкціонований обмін інформацією між абонентами може привести до одержання одним із них відомостей, доступ до яких йому заборонений. Наслідки ті ж, що й при несанкціонованому доступі.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її одержання або відправлення. Це дозволяє одній із сторін розривати укладені фінансові угоди "технічним" шляхом, формально не відмовляючись від них, наносячи тим самим другій стороні значний збиток.

Порушення інформаційного обслуговування – загроза, джерелом якої є сама ІТ. Затримка з наданням інформаційних ресурсів абонентові може призвести до тяжких для нього наслідків. Відсутність у користувача своєчасних

даних, необхідних для ухвалення рішення, може викликати його нераціональні дії.

Незаконне використання привілеїв. Будь-яка захищена система містить засоби, використовувані в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. Наприклад, на випадок раптової перевірки користувач повинен мати можливість доступу до всіх наборів системи. Зазвичай, ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користувачами, що виконують спеціальні функції. Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Звичайно, користувачі мають мінімальний набір привілеїв, а адміністратори – максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але найчастіше відбувається в процесі керування системою захисту, зокрема при недбалому користуванні привілеями. Суворе дотримання правил керування системою захисту, а також принципу мінімуму привілеїв дозволяє уникнути таких порушень. Під час опису в різній літературі різноманітних загроз для ІС і способів їх реалізації широко використовується поняття атаки на ІС.

Атака – зловмисні дії зломщика (спроби реалізації ним будь-якого виду загрози). Наприклад, атакою є застосування кожної зі шкідливих програм. Серед атак на ІС часто виділяють "маскарад" і "злом системи", які можуть бути результатом реалізації різноманітних загроз (або комплексу загроз).

Під "**маскарадом**" розуміється виконання яких-небудь дій одним користувачем ІС від імені іншого користувача. Такі дії іншому користувачеві можуть бути дозволені. Порушення полягає в присвоєнні прав і привілеїв, що називається симуляцією або моделюванням. Цілі "маскараду" – приховування яких-небудь дій за ім'ям іншого користувача або присвоєння прав і привілеїв іншого користувача для доступу до його наборів даних або для використання його привілеїв. Можуть бути й інші способи реалізації "маскараду", наприклад створення й використання програм, які в певнім місці можуть змінити певні дані, у результаті чого користувач одержує інше ім'я. "Маскарадом" називають також передачу повідомлень у мережі від імені іншого користувача. Найнебезпечніший "маскарад" у банківських системах електронних платежів, де неправильна ідентифікація клієнта може призвести до величезних збитків. Особливо це стосується платежів з використанням електронних карт. Використовуваний у них метод ідентифікації за допомогою персонального ідентифікатора досить надійний. Але порушення можуть відбуватися внаслідок помилок його використання, наприклад втрати кредитної картки або використанні очевидного ідентифікатора (свого ім'я й т. д.). Для запобігання "маскараду" необхідно використовувати надійні методи ідентифікації, блокування спроб злому системи, контроль входів у неї. Необхідно фіксувати всі події, які можуть свідчити про "маскарад", у системному журналі для його наступного аналізу. Також бажано не використовувати програмні продукти, що містять помилки, які можуть привести до "маскараду".

Під **зломом системи** розуміють навмисне проникнення в систему, коли зломщик не має санкціонованих параметрів для входу. Способи злому можуть бути різними, і при деяких з них відбувається збіг з раніше описаними загрозами. Так, об'єктом полювання часто стає пароль іншого користувача. Пароль може бути розкритий, наприклад, шляхом перебору можливих паролів. Злом системи можна здійснити також, використовуючи помилки програми входу.

Основне навантаження захисту системи від злому несе **програма входу**. Алгоритм уведення ім'я й пароля, їхнє шифрування, правила зберігання й зміни паролів не повинні містити помилок. Протистояти злому системи допоможе, наприклад, обмеження спроб неправильного уведення пароля (тобто виключити досить великий перебір) з наступним блокуванням термінала й повідомленням адміністратора у випадку порушення. Крім того, адміністратор безпеки повинен постійно контролювати активних користувачів системи: їхні імена, характер роботи, час входу й виходу й т. д. Такі дії допоможуть вчасно встановити факт злому й почати необхідні дії.

Умовою, що сприяє реалізації багатьох видів загроз ІС, є наявність "люків". **Люк-схованка**, не документована точка входу в програмний модуль, що входить до складу ПЗ ІС і ІТ. Люк вставляється в програму, звичайно, на етапі налагодження для полегшення роботи: даний модуль можна викликати в різних місцях, що дозволяє налагоджувати окремі частини програми незалежно. Наявність люка дозволяє викликати програму нестандартним чином, що може відбитися на стані системи захисту. Люки можуть залишитися в програмі з різних причин:

– їх могли забути забрати;

– для подальшого налагодження;

– для забезпечення підтримки готової програми;

– для реалізації таємного доступу до програми після її установки.

Більша небезпека люків компенсується високою складністю їх виявлення (якщо, звичайно, не знати заздалегідь про їх наявність), тому що виявлення люків – результат випадкового й трудомісткого пошуку. Захист від люків один – не допускати їхньої появи в програмі, а при прийманні програмних продуктів, розроблених іншими виробниками, варто проводити аналіз вихідних текстів програм з метою виявлення люків.

Реалізація загроз ІС приводить до різних видів прямих або непрямих втрат. **Втрати** можуть бути пов'язані з **матеріальним збитком**:

– вартість компенсації, відшкодування іншого побічно втраченого майна;

– вартість ремонтно-відбудовних робіт;

– витрати на аналіз, дослідження причин і величини збитку;

– додаткові витрати на відновлення інформації, пов'язані з відновленням роботи й контролем даних і т. д.

Втрати можуть виражатися в обмеженні банківських інтересів, фінансових витратах або у втраті клієнтури.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємозв'язку між ними, тобто з нереалізованістю системного підходу. Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

17.7. Загрози через соціальну інженерію.

Всі ми знаємо про зловмисника, який використовує свій технічний досвід для проникнення в захищені комп'ютерні системи та злому конфіденційних даних. Цей тип зловмисників постійно робить новини, спонукаючи нас протистояти їхнім подвигам, інвестуючи в нові технології, які зміцнять наш мережевий захист.

Однак є ще один тип зловмисників, які використовують різні тактики, щоб оминути наші інструменти та рішення. Їх називають "соціальними інженерами", тому що вони використовують одну слабкість, яка є в кожній організації: людська психологія. Використовуючи телефонні дзвінки та інші засоби спілкування з користувачами, ці зловмисники змушують людей передавати доступ до конфіденційної інформації організації.

Соціальна інженерія – термін, який охоплює широкий спектр шкідливих дій. Зосередимося на п'яти найпоширеніших типах атак, які використовують соціальні інженери.

1. Фішинг

Фішинг є найпоширенішим типом атаки соціальної інженерії, що відбувається сьогодні. Але що? На високому рівні більшість фішинг-шахраїв намагаються виконати три речі:

– Отримати особисту інформацію, таку як імена, адреси та номери соціального страхування.

– Використовувати скорочені або вводять в оману посилання, які перенаправляють користувачів на підозрілі веб-сайти, на яких розміщуються цільові фішингові сторінки.

– Включити погрози, страх і почуття терміновості у спробі змусити користувача реагувати якнайшвидше.

Немає двох однакових фішингових листів. Насправді існує як мінімум шість різних підкатегорій атак фішингу. Крім того, ми всі знаємо, що деякі з них погано опрацьовані, оскільки в них повідомлення страждають від орфографічних та граматичних помилок. Тим не менш, ці електронні листи зазвичай мають одну і ту ж ціль – використовувати підроблені веб-сайти або форми для крадіжки облікових даних користувача та інших особистих даних.

У нещодавній фішинг кампанії використовується скомпрометований обліковий запис електронної пошти, щоб відправити листа. У цих повідомленнях просили одержувачів переглянути запропонований документ, клацнувши вбудовану URL-адресу. Ця шкідлива URL-адреса, захищена URL-адресою Symantec для захисту від кліків, перенаправила одержувачів на зламаний обліковий запис SharePoint, який доставив другу шкідливу URL-адресу, вбудовану в документ OneNote. Цей URL, у свою чергу, перенаправляє користувачів на сторінку фішингу, що зображує портал входу в систему Microsoft Office 365.

2. Приводи

Привід – це ще одна форма соціальної інженерії, де зловмисники концентруються на створенні хорошого прийменника чи сфабрикованого сценарію, який вони використовують, щоб спробувати вкрасти особисту інформацію своїх жертв. У цих типах атак шахрай зазвичай каже, що їм потрібна певна кількість інформації від своєї мети, щоб підтвердити свою особистість. Насправді вони крадуть ці дані та використовують їх для вчинення крадіжки особистих даних або проведення вторинних атак.

Більш просунуті атаки іноді намагаються обдурити свої цілі, роблячи щось, що зловживає цифровими та/або фізичними вадами організації. Наприклад, зловмисник може видати себе зовнішнього аудитора IT-послуг, щоб він міг переконати групу фізичної безпеки цільової компанії пустити їх у будинок.

У той час як фішингові атаки в основному використовують страх і терміновість у своїх інтересах, атаки з приводом ґрунтуються на створенні хибного почуття довіри до жертви. Це вимагає від зловмисника побудувати достовірну історію, яка залишає мало місця для сумнівів із боку їхньої мети.

Привід може приймати та набуває різних форм. Незважаючи на це, багато суб'єктів загроз, які приймають цей тип атаки, вирішують маскуватися під кадри чи співробітників відділу розвитку фінансів.

3. Принада

Принада багато в чому схожа на атаки фішинга. Однак те, що відрізняє їх від інших видів соціальної інженерії, – це обіцянка будь-якого предмета чи блага, які зловмисники використовують для спокуси жертв. Приманки можуть використовувати пропозицію безкоштовного завантаження музики або фільмів, наприклад, щоб обманом змусити користувачів передати облікові дані для входу.

Зловмисники можуть також зосередитись на використанні людської цікавості за допомогою фізичних засобів.

Наприклад, ще в липні 2018 року KrebsOnSecurity повідомив про кампанію з нападу на державні установи та органи місцевого самоврядування у Сполучених Штатах. Операція розіслала китайські поштові марковані конверти, які містили заплутаний лист разом із компакт-диском (CD). Ціль полягала в тому, щоб розбудити цікавість одержувачів, щоб вони завантажували компакт-диск і тим самим ненавмисно заражали свої комп'ютери шкідливим ПЗ.

4. Що за що (quid pro quo)

Подібно до цькування, напади quid pro quo обіцяють вигоду в обмін на інформацію. Ця вигода зазвичай набуває форми послуги, тоді як цькування зазвичай набуває форми користі. Один з найбільш поширених типів атак quid pro quo, що з'явилися в останні роки, – це коли шахраї видають себе за Адміністрацію соціального забезпечення США (SSA). Ці підроблені співробітники SSA зв'язуються зі випадковими особами, повідомляють їм, що з їхнього боку виникла проблема з комп'ютером, і просять, щоб ці особи підтвердили свій номер соціального страхування, все це спрямоване на крадіжку особистих даних. В інших випадках, виявлених Федеральною торговою комісією (FTC), зловмисники створюють підроблені веб-сайти SSA, які кажуть, що можуть допомогти користувачам подати заявку на нові карти соціального

забезпечення, але натомість просто крадуть їхню особисту інформацію.

Тим не менш, важливо відзначити, що зловмисники можуть використовувати пропозиції quid pro quo, які набагато менш витончені, ніж хитрощі на тему SSA. Як показали попередні атаки, офісні працівники більш ніж готові віддати свої паролі за дешеву ручку або навіть плитку шоколаду.

5. Хвостовик (Tailgating)

Наш останній тип соціальної атаки на сьогоднішній день відомий як Tailgating. У цих типах атак хтось без належної автентифікації слідує за перевіреним співробітником в обмежену область. Зловмисник може видати себе за водія служби доставки та почекати зовні будівлі, щоб розпочати роботу. Коли співробітник отримує схвалення служби безпеки та відчиняє двері, зловмисник просить співробітника притримати двері, тим самим одержуючи доступ до будівлі. Tailgating не працює у всіх корпоративних умовах, таких як великі компанії, входи до яких вимагають використання карти-ключа. Однак на середніх підприємствах зловмисники можуть зав'язати розмову зі співробітниками та використати цю демонстрацію знайомства, щоб обійти стійку реєстрації. Фактично, Колін Грінлес, консультант з безпеки в Siemens Enterprise Communications, використав цю тактику, щоб отримати доступ до кількох поверхів і кімнат даних у фінансовій компанії, зареєстрованій на біржі FTSE. Він навіть зміг відкрити магазин у залі засідань на третьому поверсі та працювати там протягом кількох днів.

Рекомендації щодо соціальної інженерії

Зловмисники, які беруть участь в атаках соціальної інженерії, полюють на людську психологію та цікавість, щоб поставити під загрозу інформацію. Пам'ятаючи про цей фокус, орієнтований на людину, організації повинні допомогти своїм співробітникам протистояти атакам такого типу.

Ось кілька порад, які організації можуть включити до своїх навчальних програм безпеки, які допоможуть користувачам уникнути схем соціальної інженерії:

– Не відкривайте листи з ненадійних джерел. Зв'яжіться з другом або членом сім'ї особисто або по телефону, якщо ви отримали від них підозрілі повідомлення.

– Не вірте реченням від незнайомих людей. Сумнівайтесь! Якщо пропозиції здаються надто хорошими, щоб бути правдою, вони, мабуть, це шахрайство.

– Заблокуйте свій ноутбук, коли ви залишаєтеся робоче місце.

– Купити антивірусне програмне забезпечення. Жодне AV-рішення не може захистити від будь-якої загрози, яка ставить під загрозу інформацію користувачів, але вони можуть допомогти захистити від деяких атак.

– Прочитайте політику конфіденційності компанії, щоб зрозуміти, за яких обставин ви можете або повинні впустити незнайомця в будівлю.