Основні види і джерела атак на інформацію

Сучасна ситуація в області інформаційної безпеки

При зберіганні, підтримці і наданні доступу до будь-якого інформаційного об'єкту його власник, або уповноважена їм особа, накладає явно або самоочевидний набір правив по роботі з нею. Навмисне їх порушення класифікується як атака на інформацію.

З масовим впровадженням комп'ютерів у всі сфери діяльності людини обсяг інформації, що зберігається в електронному вигляді виріс в тисячі раз. І тепер скопіювати за півхвилини дискету з файлом, що містить план випуску продукції, набагато простіше, ніж копіювати або переписувати купу паперів. З появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

Можливими наслідками атак на інформацію в першу чергу, є економічні втрати:

1. Розкриття комерційної інформації може привести до серйозних прямих збитків на ринку
2. Звістка про крадіжку великого обсягу інформації звичайно серйозно впливає на репутацію фірми, ведучи побічно до втрат в обсягах комерційних операцій
3. Фірми-конкуренти можуть скористатися крадіжкою інформації, якщо та залишилася непоміченою, для того, щоб повністю розорити фірму, нав'язуючи їй фіктивні або явно збиткові операції
4. Підміна інформації як на етапі передачі, так і на етапі зберігання у фірмі може привести до величезних збитків
5. Багаторазові успішні атаки на фірму, що надає який-небудь вид інформаційних послуг, знижують довіру до фірми у клієнтів, що позначається на розмірі прибутків

Також, комп'ютерні атаки можуть принести і величезний моральний збиток. Жодному користувачу комп'ютерної мережі не хочеться, щоб його листи окрім адресата одержували ще 5-10 чоловік, або, наприклад, весь текст, що набирається на клавіатурі ЕОМ, копіювався в буфер, а потім при підключенні до Інтернету відправлявся на певний сервер, як це відбувається в тисячах і десятках тисяч випадків.

Згідно матеріалів статистичних досліджень, кожний десятий випадок пошкодження електронних даних пов'язаний з комп'ютерними атаками. Виконавцем цих дій були: в 81% випадків – поточний кадровий склад установ, тільки в 13% випадків – повністю сторонні люди, і в 6% випадків – колишні працівники цих же установ. Частка атак, виконуємих співробітниками фірм і підприємств, примушує застосовувати не тільки про технічних, але і про психологічні методи профілактики подібних дій. Діставшись до інформації: в 44% випадків атак були зроблені безпосередні крадіжки грошей з електронних рахунків, в 16% випадків виводилося з ладу програмне забезпечення, так же часто – в 16% випадків – здійснювалася крадіжка інформації з різними наслідками, в 12% випадків інформація була сфальсифікована, в 10% випадків зловмисники за

допомогою комп'ютера скористалися або замовили послуги, до яких у принципі не повинні мати доступу.

Категорії інформаційної безпеки

Інформація з погляду інформаційної безпеки володіє наступними категоріями:

- конфіденційність – гарантія того, що конкретна інформація доступна тільки, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації
- цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення
- автентичність – гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення
- апеллюємість – гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора, хтось інший намагається заявити, що він автор повідомлення, а при порушенні апеллюємості – сам автор намагається "відхреститися" від своїх слів, підписаних їм одного разу.

Відносно інформаційних систем застосовуються інші категорії :

- надійність – гарантія того, що система поводиться в нормальному і позаштатному режимах так, як заплановано
- точність – гарантія точного і повного виконання всіх команд
- контроль доступу – гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються
- контрольованість – гарантія того, що у будь-який момент може бути проведена повноцінна перевірка будь-якого компоненту програмного комплексу
- контроль ідентифікації – гарантія того, що клієнт, підключений в даний момент до системи, є саме тим, за кого себе видає
- стійкість до умисних збоїв – гарантія того, що при умисному внесенні помилок в межах заздалегідь обумовлених норм система поводитиметься так, як обумовлено заздалегідь.

Термінали захищеної інформаційної системи

Термінали – це точки входу користувача в інформаційну мережу. У тому випадку, коли до них мають доступ декількох чоловік або взагалі будь-хто, при їх проектуванні і експлуатації необхідне ретельне дотримання цілого комплексу заходів безпеки

Найпоширенішим способом входу в систему при атаках на інформацію залишається вхід через офіційний log-in запит системи. Обчислювальна техніка, яка дозволяє реалізувати вхід в систему, називається в теорії інформаційної безпеки терміналом. Якщо система складається всього з одного персонального комп'ютера, то він одночасно вважається і терміналом і сервером. Доступ до терміналу може бути фізичним, у тому випадку, коли термінал – це ЕОМ з клавіатурою і дисплеєм, або видаленим – найчастіше по телефонній лінії (в цьому випадку терміналом є модем, підключений або безпосередньо до системи, або до її фізичного терміналу).
При використанні терміналів з фізичним доступом необхідно дотримувати наступні вимоги:

1. Захищеність терміналу повинна відповідати захищеності приміщення: термінали без пароля може бути присутнім тільки в тих приміщеннях, куди мають доступ обличчя відповідного або вищого рівня доступу. Відсутність імені реєстрації можлива тільки в тому випадку, якщо до терміналу має доступ тільки одна людина, або якщо на групу осіб, що мають до нього доступ, розповсюджуються загальні заходи відповідальності. Термінали, встановлені в публічних місцях повинні завжди запрошувати ім'я реєстрації і пароль.
2. Системи контролю за доступом в приміщення зі встановленим терміналом повинні працювати повноцінно і відповідно до загальної схеми доступу до інформації.
3. У випадку установки терміналу в місцях з широким скупченням народу клавіатура, а якщо необхідно, то і дисплей повинні бути обладнані пристроями, що дозволяють бачити їх тільки працюючому в даний момент клієнту (непрозорі скляні або пластмасові огорожі, шторки, "втоплена" модель клавіатури).

При використанні видалених терміналів необхідно дотримувати наступні правила:

1. Будь-який видалений термінал повинен запрошувати ім'я реєстрації і пароль.
2. Своєчасне відключення всіх модемів, не потрібних в даний момент фірмі або не контрольованих в даний момент співробітниками.
3. По можливості рекомендується використовувати схему зворотного дзвінка від модему, оскільки вона гарантує з рівнем надійності АТС те, що видалений клієнт дістав доступ з певного телефонного номера.
4. З log-in запиту терміналу рекомендується прибрати всі безпосередню інформацію щодо імені фірми, її логотипу і т.п. – це не дозволить комп'ютерним злочинцям, що просто перебирають номери з модемами, дізнатися log-in екран якої фірми вони знайшли.
5. На вході в систему рекомендується виводити на екран попередження про те, що вхід в систему без повноважень на це переслідується згідно із законом. Це стане ще одним застереженням зловмисникам, а також, буде надійним

аргументом на користь атакованої фірми в судовому розгляді, якщо таке проводитиметься.

Безвідносно від фізичного або комутованого доступу до терміналу, лінія, що з'єднує термінал (комутований, або встановлений в публічному місці) із зоною ядра інформаційної системи повинна бути захищена від прослуховування, або ж весь обмін інформацією повинен здійснюватись за конфіденційною схемою ідентифікації і надійною схемою аутентифікації клієнта.

Подальші дії зловмисника, що дістав доступ до термінальної точки входу, можуть розвиватися по двох основних напрямах: спроби з'ясування пароля прямо або побічно; спроби входу в систему вчинено без знання пароля, ґрунтуючись на помилках в реалізації програмного або апаратного забезпечення.
Перебір паролів по словнику був якийсь час однією з найпоширенішої техніки підбору паролів. Сьогодні набули широке поширення мови складання паролів, що записують в абстрактній формі основні принципи складання паролів середньостатистичними користувачами ЕОМ.
Іншою модифікацією підбору паролів є перевірка паролів, встановлюваних в системах за умовчанням. В деяких випадках адміністратор програмного забезпечення, проїнсталювавши або отримавши новий продукт від розробника, не спромагається перевірити, з чого складається система безпеки. Як наслідок, пароль, встановлений у фірмі розробнику за умовчанням, залишається основним паролем в системі. В мережі Інтернет публікуються величезні списки паролів за умовчанням практично до всіх версій програмного забезпечення, якщо вони встановлюються на ньому виробником.
Основні вимоги до інформаційної безпеки, засновані на аналізі даного методу, наступні:

1. Вхід всіх користувачів в систему повинен підтверджуватися введенням унікального для клієнта пароля.
2. Пароль повинен ретельно підбиратися так, щоб його інформаційна місткість відповідала часу повного перебору пароля. Для цього необхідно детально інструктувати клієнтів про поняття "простий до підбору пароль", або передати операцію вибору пароля у ведення інженера по безпеці.
3. Паролі за умовчанням повинні бути змінені до офіційного запуску системи і навіть до скільки або публічних випробувань програмного комплексу. Особливо це відноситься до мережного програмного забезпечення.
4. Всі помилкові спроби увійти до системи повинні враховуватися, записуватися у файл журналу подій і аналізуватися через "розумний" проміжок часу. Якщо в системі передбачена можливість блокування клієнта або всієї системи після певної кількості невдалих спроб входу, цією можливістю необхідно скористатися. Зазвичай необхідно блокувати клієнта після 3-їй підряд неправильної спроби набору пароля, і, відповідно, блокувати систему після наступної кількості невдалих спроб входу за деякий період (годину, зміну, доба):

$$K=\max(\text{int}(N*0.1*3)+1, 3),$$

де N – середня кількість клієнтів, що підключаються за цей період до системи 0.1 – 10% межа "забудькуватості пароля", 3 – ті ж самі три спроби на згадку пароля.

Інформація про блокування клієнта або системи повинна автоматично поступати на пульт контролю за системою.

5. У момент відправки пакету підтвердження або відкидання пароля в системі повинна бути встановлена затримка (2 - 5 секунд). Це не дозволить зловмиснику, потрапивши на лінію з добрим зв'язком до об'єкту атаки перебирати по сотні тисяч паролів за секунду.
6. Всі дійсні в системі паролі бажано перевіряти сучасними програмами підбору паролів, або оцінювати особисто адміністратору системи.
7. Через певні проміжки часу необхідна примусова зміна пароля у клієнтів. Інтервалами зміни пароля, що найчастіше використовуються, є рік, місяць і тиждень (залежно від рівня конфіденційності інформації і частоти входу в систему).
8. Всі невживані протягом довгого часу імена реєстрації повинні переводитися в закритий (недосяжний для реєстрації) стан. Це відноситься до співробітників, що знаходяться у відпустці, на лікарняному, у відрядженні, а також до імен реєстрації, створених для тестів, випробувань системи і т.п.
9. Від співробітників і всіх операторів терміналу необхідно вимагати суворе нерозголошування паролів, відсутність яких-небудь взаємозв'язків пароля з широковідомими фактами і даними, і відсутність паперових записів пароля "через погану пам'ять".

Наступною по частоті використання є методика отримання паролів з самої системи. Основними двома можливостями з'ясування пароля є несанкціонований доступ до носія, що містить їх, або використання недокументованих можливостей і помилок в реалізації системи.

Перша група методів заснована на тому, що будь-якій системі доводиться де-небудь зберігати оригінали паролів всіх клієнтів для того, щоб звіряти їх у момент реєстрації. При цьому паролі можуть зберігатися як у відкритому текстовому вигляді, як це має місце в багатьох клонах UNIX, так і представлені у вигляді малозначних контрольних сум (хеш - значень), як це реалізовано в ОС Windows, Novell NetWare і багатьох інших. При цьому для зберігання паролів на носії не може бути використана основна методика захисту – шифрування. Якщо всі паролі зашифровані яким-небудь ключем, то цей ключ теж повинен зберігатися в самій системі для того, щоб вона працювала автоматично, не питаючи кожного разу у адміністратора дозвіл. Тому, дістався доступ до подібної інформації, зловмисник може або відновити пароль в читабельному вигляді, або відправити запити, підтверджені даним хеш - значенням, не відновляю його. Рекомендації ж по запобіганню розкраданням паролів полягають в перевірці чи не доступний файл з паролями, або таблиця в базі даних, що зберігає ці паролі, декому ще окрім адміністраторів системи, чи не створюється системою резервних файлів, в місцях доступних іншим користувачам і т.п. . Оскільки крадіжка паролів є найгрубішим вторгненням в систему, розробники надають їй досить пильну увагу, і дотримання

всіх рекомендацій по використовуванню системи звичайно достатньо для запобігання подібним ситуаціям.

Отримання доступу до паролів завдяки недокументованим можливостям систем зустрічається украй рідко. Раніше ця методика використовувалася розробниками набагато частіше в основному в цілях відладки, або для екстреного відновлення працездатності системи. Але поступово з розвитком як технологій зворотної компіляції, так і інформаційної зв'язаності миру вона поступово стала зникати. Будь-які недокументовані можливості рано чи пізно стають відомими, після чого новина про це облітає світ і розробникам доводиться розсилати всім користувачам скомпрометованої системи "програмні латочки" або нові версії програмного продукту. Єдиною мірою профілактики цього методу є постійний пошук на серверах, присвячених комп'ютерній безпеці, оголошень про всі неприємності з програмним забезпеченням, встановленим у КСОІ. Будь-яка подібна вбудована можливість може понизити на порядок загальну безпеку системи, як би добре вона не була завуальована в коді програмного продукту.

Наступною поширеною технологією отримання паролів є копіювання буфера клавіатури у момент набору пароля на терміналі. Цей метод використовується рідко, так для нього необхідний доступ до термінальної машини з можливістю запуску програм. Але якщо зловмисник все-таки дістає подібний доступ, дієвість даного методу дуже висока:

1. Робота програми - перехоплювача паролів (так званого "троянського коня") на робочій станції непомітна.

2. Подібна програма сама може відправляти результати роботи на наперед заданий сервер або анонімним користувачам, що різко спрощує саму процедуру отримання паролів хакером, і утрудняє пошук і доказ його провини.

Двома основними методами боротьби з копіюванням паролів є:

1. адекватний захист робочих станцій від запуску сторонніх програм:

   а) відключення змінних носіїв інформації,

   б) спеціальні драйвера, що блокують запуск здійснимих файлів без відома оператора, або адміністратора,

   в) монітори, що повідомляють про будь-які зміни системних настройок і списку програм, що автоматично запускаються,

2. система одноразових паролів (при кожній реєстрації в системі клієнтам з дуже високим рівнем відповідальності самою системою генерується новий пароль).

Сканування сучасними антивірусними програмами також може допомогти у виявленні "троянських" програм, але тільки тих з них, які набули широке поширення.

Наступний метод отримання паролів відноситься тільки до мережевого програмного забезпечення. В багатьох програмах не враховується можливість перехоплення будь-якої інформації, що йде по мережі – так званого мережевого трафіку. Більше половини протоколів мережі Інтернет передають паролі в

нешифрованому вигляді – відкритим текстом. До них відносяться протоколи передачі електронної пошти SMTP і POP3, протокол передачі файлів FTP, одна з схем авторизації на WWW-серверах.

Сучасне апаратне і програмне забезпечення дозволяє одержувати всю інформацію, що проходить по сегменту мережі, до якого підключений конкретний комп'ютер, і аналізувати її в реальному масштабі часу. Можливі декілька варіантів прослуховування трафіку:

1) це може зробити службовець компанії з свого робочого комп'ютера,

2) зловмисник, що підключився до сегменту за допомогою портативної ЕОМ або мобільнішого пристрою,

3) трафік, що йде по мережі Інтернет, технічно може прослуховуватися з боку безпосереднього провайдера, з боку будь-якої організації, що надає транспортні послуги для мережі Інтернет (листування усередині країни в середньому йде через 3-4 компанії, за межі країни – через 5-8).

Для комплексного захисту від подібної можливості крадіжки паролів необхідно виконувати наступні заходи:

1. Фізичний доступ до мережних кабелів повинен відповідати рівню доступу до інформації.
2. При визначенні топології мережі слід уникати при будь-якій нагоді широкомовних топологій. Оптимальною одиницею сегментації є група операторів з рівними правами доступу, або якщо ця група складає більше 10 чоловік, то кімната або відділ усередині групи. У жодному випадку на одному кабелі не повинні знаходитися оператори з різними рівнями доступу, якщо тільки весь передаваний трафік не шифрується, а ідентифікація не виконується по прихованій схемі без відкритої передачі пароля.
3. До всіх інформаційних потоків, що виходять за межі закладу, повинні застосовуватися ті ж правила, що стосуються об'єднання різнорівневих терміналів.

Соціальна психологія і інші способи отримання паролів

Іноді зловмисники вступають і в прямий контакт з лицями, що володіють потрібною їм інформацією, розігруючи досить переконливі сцени. "Жертва" омани, що повірила в реальність розказаної їй по телефону або в електронному листі ситуації, сама повідомляє пароль зловмиснику.
Розглянемо декілька методів, що досить часто зустрічаються.
Дзвінок адміністратору – зловмисник вибирає із списку співробітників того, хто не використовував пароль для входу протягом декількох днів (відпустка, відгули, відрядження) і кого адміністратор не знає по голосу. Потім слідує дзвінок з

поясненням ситуації про забутий пароль, проханням зачитати пароль, або змінити його на новий.
Майже така ж схема, але у зворотний бік може бути розіграна зловмисником на адресу співробітника – дзвінок від адміністратора. В цьому випадку він представляється вже співробітником служби інформаційної безпеки і просить назвати пароль або через збій, що відбувся, в базі даних, або нібито для підтвердження особи самого співробітника з якої-небудь причини, або з приводу останнього підключення співробітника до якого-небудь інформаційного серверу усередині закладу. Крім того, така схема може бути проведена і без телефонного дзвінка – по електронній пошті, що неодноразово і виконувалося нібито від імені поштових і Web-серверов в мережі Інтернет.
Обидва даних методу відносяться до групи "атака по соціальній психології" і можуть приймати самі різні форми. Їх профілактикою може бути тільки ретельне роз'яснення всім співробітникам, в особливо важливих випадках введення адміністративних заходів і особливого регламенту запиту і зміни пароля.
Необхідно ретельно інструктувати співробітників про небезпеку залишення робочих станцій, не закритих паролем. В першу чергу це, звичайно, відноситься до терміналів, що працюють в публічних місцях і офісах з нижчим рівнем доступу до інформації, проте, і при роботі в приміщеннях з рівним рівнем доступу не рекомендується давати можливість співробітникам працювати за іншими ЕОМ тим більше у відсутність власника. Як програмні профілактичні заходи використовуються екранні заставки з паролем, що з'являються через 5-10 хвилин відсутності робочої активності, автоматичне відключення сервером клієнта через такий же проміжок часу.
Велика увага слідує уділяти будь-яким носіям інформації, що покидають межі закладу. Найчастішими причинами цього бувають ремонт апаратури і списання технологічно застарілої техніки. На робочих поверхнях носіїв навіть у видалених областях знаходиться інформація, яка може представляти або безпосередній інтерес, або побічно послужити причиною вторгнення в систему. При використанні віртуальної пам'яті частина вмісту ОЗП записується на жорсткий диск, що теоретично може привезти навіть до збереження пароля на постійному носії. Ремонт за місцем роботи, повинен проводиться під контролем інженера із служби інформаційної безпеки. Всі носії інформації, що покидають заклад повинні надійно чиститися або знищуватися механічно (залежно від подальших цілей їх використовування).
На сьогоднішній день не існує розумних за критерієм "ціна/надійність" носіїв інформації, не доступних до втручання. Будова файлів, їх заголовки і розташування в будь-якій операційній системі може бути прочитане при використанні відповідного програмного забезпечення. Практично нерозкриваним може бути тільки незалежний носій, що автоматично руйнує інформацію при спробі несанкціонованого підключення до будь-яких точок, окрім дозволених роз'ємів, що бажано саморуйнується при розгерметизації, що має всередині мікропроцесор, що аналізує пароль по схемі без відкритої передачі.
Для приватного листування ця проблема розв'язується набагато простіше і дешевше – за допомогою криптографії. Будь-який об'єм інформації будучи зашифрований за допомогою більш менш стійкої криптосистеми, недосяжний для прочитання без знання ключа. Абсолютно не важливо, зберігається він на

жорсткому диску, на дискеті або компакт-диску, не важливо під управлінням якої операційної системи.