Тема 9. Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями.

Управління паролями

Паролі - це ключі, які відкривають доступ до особистих даних, що зберігаються на комп'ютері та в облікових записах в Інтернеті.

Якщо зловмисники вкрадуть ці дані, вони можуть скористатися ними для відкриття нових рахунків кредитних карт, отримання кредиту або виконання через Інтернет інших дій від вашого імені. Дуже часто ви можете не підозрювати про такі дії до тих пір, поки не стане занадто пізно.

З величезною кількістю системних паролів та сайтів, доступ до яких надається лише зареєстрованим користувачам, неможливо запам'ятати всі пари «ім'я користувача / пароль», якщо тільки ви не використовуєте одні й ті самі ім'я та пароль для всіх облікових записів або не записуєте їх. Обидва ці методи мають зниженим рівнем безпеки.

Той, хто використовує одні й ті ж ім'я користувача та пароль, починаючи електронною поштою і закінчуючи особистими банківськими рахунками, надають повний доступ до власного життя кожному, хто зможе зламати один з використовуваних акаунтів, так як таким чином, зловмисники зможуть використовувати отримані дані для будь-яких інших облікових записів. Отримати доступ до важливої інформації можна через файли cookie, які зберігаються на комп'ютері (це залежить від ступеня уразливості використовуваного браузера), і за допомогою сайтів, які не можуть використовувати протокол http або технологію SSL (відкритий стандарт для створення безпечних каналів підключення, які запобігають витік важливих конфіденційних відомостей, таких як номери кредитних карт). В даному випадку, ваші ім'я користувача та пароль виявляються у відкритому доступі в Інтернеті і можуть бути отримані будь-якою кількістю комп'ютерів.

При записуванні ім'я користувача та пароль на папір завжди існує можливість втратити цей листок, або хто-небудь може знайти його і отримати доступ до ваших акаунтів. Ймовірність такої загрози значно зростає, якщо ви залишаєте листок з даними під клавіатурою, приклеюєте його на монітор, ноутбук або просто залишаєте його на столі. Пароль використовується для забезпечення безпеки комп'ютерних програм, і тому, записуючи його на папір, ви просто видаляєте всяку безпеку. З іншого боку, ім'я користувача та пароль можуть бути легко викрадені, якщо вони надсилаються через Інтернет відкритим текстом, але зазвичай ті користувачі, які записують дані на папір для різних акаунтів, використовують різні паролі. Тому при втраті листка з паролем вони не втратять контроль над усіма обліковими записами.

Одним з кращих способів забезпечити безпеку при відкритті акаунтів є використання різних ім'я користувача та пароль при кожній реєстрації. Запам'ятати їх буває дуже складно (тому часто використовуються методи, описані вище). Все ж існує кращий спосіб збереження паролів - використання інструменту управління паролями. Таким чином, значно спрощується збереження паролів для кожного облікового запису. Іншою важливою перевагою використання менеджера паролів є те, що можна використовувати безпечніші паролі і не боятися забути їх.

Існує безліч менеджерів паролів, доступних в Інтернеті, - деякі платні, інші безкоштовні. Вибір типу програм залежить від користувача.

Менеджер паролів - програмне забезпечення, яке допомагає користувачеві працювати з паролями і PIN-кодами. У подібного програмного забезпечення зазвичай є в наявності місцева база даних або файли, які містять зашифровані дані пароля. Багато менеджерів паролів також працюють як заповнювач форми, тобто вони заповнюють поле користувач і дані пароля автоматично в формах. Зазвичай вони реалізовані як розширення браузера.

Менеджери паролів діляться на три основні категорії:

Десктоп - зберігають паролі до програмного забезпечення, встановленого на жорсткому диску комп'ютера.

Портативні - зберігають паролі до програмного забезпечення на мобільних пристроях, таких як КПК, смартфон або до портативних додатків на USB флеш-накопичувачі.

Мережеві - менеджери паролів онлайн, де паролі збережені на веб-сайтах провайдерів.

Менеджери паролів можуть також використовуватися як захист від фішингу. На відміну від людей, програма менеджер паролів може звертатися з автоматизованим скриптом логіна не сприйнятливі до візуальних імітацій, які схожі на веб-сайти. З цією вбудованою перевагою використання менеджера паролів вигідно, навіть якщо у користувача є всього кілька паролів, які він пам'ятає. Однак не всі менеджери паролів можуть автоматично звертатися з більш складними процедурами ідентифікації, накладеними багатьма банківськими веб-сайтами.

Менеджери паролів зазвичай використовують вибраний користувачем основний пароль, або секретну фразу (passphrase), щоб сформувати ключ, використовуваний для зашифровки збережених паролів. Цей основний пароль повинен бути досить складним, щоб встояти при атаках зловмисників (наприклад повний перебір).

Якщо основний пароль буде зламаний, то будуть розкриті всі збережені в базі даних програми паролі. Це демонструє зворотний зв'язок між зручністю використання і безпекою: єдиний пароль може бути більш зручний, але якщо він буде зламаний, то поставить під загрозу всі збережені паролі.

Основний пароль може також бути атакований і виявлений при використанні кейлоггера або акустичного криптоаналізу (acoustic cryptanalysis). Така загроза може бути знижена шляхом використання віртуальної клавіатури, як, наприклад, в KeePass.

Деякі менеджери паролів включають генератор паролів. Згенеровані паролі можуть бути відгадувати, якщо менеджер пароля не використовує криптографічно безпечний генератор випадкових чисел.

Онлайн менеджер паролів - веб-сайт, який надійно зберігає дані логіна. Таким чином це мережева версія звичайного десктоп-менеджера паролів.

Переваги онлайн менеджерів паролів над десктоп-версіями - це мобільність (вони можуть використовуватися на будь-якому комп'ютері з web-браузером і інтернет-з'єднанням, без необхідності встановлювати програмне забезпечення) і менший ризик втрати паролів через злодійство або пошкодження PC. Ризик пошкодження може бути в значній мірі знижений, якщо заздалегідь будуть створені резервні копії.

Головний недолік онлайн менеджерів паролів - необхідна довіра хостингу сайту. Неодноразові зломи і втрати централізовано збереженої інформації на сервері не вселяють довіри.

Існують змішані рішення. Ряд ресурсів, таких як FortNotes або МоіПаролі, що надають послуги онлайн-зберігання паролів та інших секретних даних, поширюють вихідні коди цих систем. Можливість провести аудит коду та встановити таку систему на захищений фаєрволом сервер або на сервер, що не має прямий вихід в Інтернет, дозволяє вирішити проблему з можливою компрометацією даних.

Використання мережевого менеджера паролів - альтернатива технології єдиного входу (Single Sign On), такий як OpenID або Microsoft's Windows Live ID, і може використовуватися як тимчасова міра, поки не буде прийнятий кращий метод.

Також існує менеджери паролів з бар'єрним захистом. У цьому випадку захищається інтернет-аккаунт користувача в цілому. Периметр захисту будується починаючи від протидії клавіатурним і екранним шпигунам, і закінчуючи захистом від підміни ip-адреси мережевого ресурсу. Прикладом є Keepy Internet Password Security. Для мережевого захисту використовується Google Public DNS, а протидія шпигунам забезпечується автоматичною підстановкою авторизаційних даних в web-форми.

Правила роботи з паролями.

Для зловмисника най надійний пароль виглядає як випадковий набір знаків. Наступні критерії допоможуть в виборі пароля.

Використовуйте якомога більше символів. Кожен додатковий знак збільшує ступінь захисту пароля. Пароль повинен містити не менш 8 знаків; 14 знаків і більше є ідеальним варіантом.

Так як багато систем дозволяють використовувати знак пробілу при створенні пароля, можна скласти пароль з декількох слів - парольний фразу. Такі фрази легше запам'ятати і важче підібрати.

Використовуйте комбінацію з літер, цифр та інших символів. Чим більше різних знаків містить пароль, тим важче його підібрати. Інші важливі відомості:

Чим менше різних символів ви використовуєте, тим довше повинен бути ваш пароль. Пароль з 15 випадково вибраних літер і цифр приблизно в 33 тисячі разів надійніше, ніж пароль з 8 знаків, що містить різні типи наявних на клавіатурі знаків. Якщо немає можливості включити в пароль символи, слід зробити його значно довше, щоб забезпечити ту ж ступінь захисту. Ідеальний пароль поєднує в собі довжину і різноманітність знаків.

Використовуйте всі символи клавіатури, А не тільки часто використовувані. Цифри і символи, що вводяться за допомогою клавіші Shift, також часто використовуються при створенні паролів. Пароль буде надійніше, якщо ви використовуєте всі наявні на клавіатурі символи, включаючи знаки пунктуації, розташовані не в верхньому ряду клавіатури, і символи, характерні тільки для вашої мови.

Використовуйте слова і фрази, легкі для запам'ятовування, але не очевидні для зловмисників. Найпростіше запам'ятати паролі і парольні фрази, записавши їх. Всупереч загальноприйнятій думці, немає нічого страшного в записі пароля, якщо дані при цьому захищені належним чином.

Паролі, записані на папері, звичайно важче зламати через Інтернет, ніж паролі, що зберігаються в диспетчері паролів, на веб-сайті або в іншій програмі для зберігання даних.

Шість етапів створення надійного пароля що легко запам’ятовується

1. Придумайте речення, яке точно не забудете, Ця пропозиція і буде основою для надійного пароля або парольного фрази. Пропозиція повинна бути незабутнім (наприклад, "Моєму синові Павлу три роки").
2. Переконайтеся, що обрана вами система перевірки пароля допускає використання ідентифікаційних фраз. Якщо є можливість використовувати парольну фрази (з пробілами між знаками), скористайтеся нею.
3. Якщо використання ідентифікаційних фраз недопустимо в даній системі, скористайтеся звичайним паролем. Складіть нове безглузде слово з перших букв усіх слів, що входять до створеного пропозицію. У нашому прикладі вийде: "мсптг".
4. Ускладните комбінацію, Використовуючи великі літери, малі літери і цифри. Можна поміняти місцями букви в слові або навмисно допустити орфографічні помилки. Наприклад, в парольного фразі, наведеній вище, можна допустити помилку в імені або замінити слово "три" на цифру 3. Є безліч можливих підстановок, і чим довше пропозицію, тим більш надійним буде пароль. Наш приклад можна перетворити так: "Моєму синові Па8лУ 3 року". Якщо комп'ютер або система не підтримують парольні фрази, той же метод можна застосувати і до простого паролю. Наприклад, "мСп3Г".
5. Нарешті, замініть окремі символи. Можна використовувати знаки, схожі на літери, об'єднувати слова (видаляючи пробіл між ними) і т. п. Дотримуючись нашого прикладу, ми отримуємо: "Моєму $ иНуП @ в8лУ 3 року" або "м $ п3Г!".
6. Перевірте свій новий пароль за допомогою програми перевірки паролів. Програма перевірки паролів на цьому веб-сайті визначить надійність вибраного пароля, як тільки ви його введете і не збережете при цьому.

Методи створення пароля, які не слід використовувати.

Вище ми розглянули як створити надійний пароль. Тепер розглянемо те, що не потрібно робити при підборі надійних паролів. Існують загальноприйняті методи, про які можуть знати і зловмисники. Щоб уникнути створення ненадійного пароля: не використовуйте послідовні комбінації і повторювані символи. Такі поєднання (наприклад, "12345678", "222222", "abcdefg" або поєднання сусідніх букв на клавіатурі) не є надійними паролями.

Уникайте використання тільки замін схожих цифр і символів. Злочинців та інших зловмисників, що володіють достатніми знаннями для підбору і злому пароля, не вдасться ввести в оману подібними замінами, наприклад "i" на "1" або "a" на "@" в словах "M1cr0 $ 0ft" або "П @ р0ль ". Однак не варто нехтувати такими замінами в поєднанні з іншими методами підвищення надійності пароля, такими як збільшення довжини, неправильне написання, використання великих і малих букв.

Не застосовуйте своє ім'я користувача в якості пароля. Уникайте також використання інших

особистих даних (своїх або своїх близьких), таких як ім'я, дата народження, код соціального страхування і т. д. Ці відомості використовуються зловмисниками в першу чергу.

Уникайте словникових слів на будь-якій мові. Зловмисники володіють досконалими засобами, що дозволяють швидко підібрати паролі, в основі яких лежать слова з різних мов; слова, написані задом наперед; поширені орфографічні помилки і заміни, а також всі види лайки та інших слів, які не вимовляють при дітях.

Використовуйте кілька паролів. При зломі одного комп'ютера або системи, де використовується певний пароль, небезпеки піддаються всі інші дані, захищені тим же паролем. Настійно рекомендується використовувати різні паролі для різних систем.

Не зберігайте пароль в Інтернеті. Зловмисник, який отримав доступ до вашого паролю в Інтернеті або в комп'ютерній мережі, отримує доступ до всіх даних.

Використання порожнього пароля

Порожній пароль (відсутність пароля) більш ефективний, ніж ненадійний, такий як, наприклад, "1234". Простий пароль легко розгадати, але на комп'ютерах з Windows XP до облікового запису, не захищеної паролем, не можна отримати доступ через локальну мережу або Інтернет (недоступна в ОС Microsoft Windows 2000, Windows Me і в більш ранніх версіях). Порожній пароль для облікового запису на комп'ютері можна використовувати, якщо виконані перераховані нижче вимоги.

У вас один або кілька комп'ютерів, але вам не потрібен доступ з одного комп'ютера на інший.

Ваш комп'ютер фізично захищений (ви довіряєте всім, хто має доступ до вашого комп'ютера).

Не завжди рекомендується використовувати порожній пароль. Наприклад, переносний комп'ютер швидше за все фізично не захищений, і на ньому краще використовувати самий надійний пароль.

Облікові записи в Інтернеті

Веб-сайти мають різні політики, що регулюють доступ до облікового запису і зміна пароля. На домашній сторінці веб-сайту знайдіть посилання (наприклад "Рахунок"), що служить для переходу на сторінку веб-сайту, де виконується управління паролем і обліковим записом.

Паролі на комп'ютері

Відомості про створення і зміну облікових записів, захищених паролями, а також про доступ до них і про те, як встановити захист паролем при завантаженні комп'ютера, зазвичай маються на файлах довідки операційної системи. Можна також спробувати знайти ці відомості на веб-сайті виробника програмного забезпечення. Наприклад, в ОС Microsoft Windows XP відомості про управлінні паролями, їх зміну і т. д. можна знайти в системі інтерактивної довідки.

Зберігання паролів в секреті

Ставтеся до паролів та парольним фразам так само серйозно, як до даних, які вони захищають.

Нікому не повідомляйте пароль. Тримайте пароль в секреті від своїх близьких (особливо від дітей) та друзів, які можуть повідомити його кому-небудь ще. Винятком є паролі, які необхідно знати вашим близьким, наприклад пароль до вашого банківського рахунку в Інтернеті, який можна повідомити дружині або чоловікові.

Ніколи не пересилайте пароль по електронній пошті. Будь-яке повідомлення електронної пошти, що містить запит пароля або вимагає перейти на веб-сайт для підтвердження пароля, майже напевно є шахрайським. Це відноситься і до повідомлень такого типу, отриманим від надійної компанії або людини. Повідомлення електронної пошти може бути перехоплено, а відправник запиту може бути зовсім не тим, за кого себе видає. В фішинг-аферах використовуються шахрайські повідомлення електронної пошти, обманним шляхом змушують розкрити ім'я користувача та пароль і дозволяють зловмисникам заволодіти ідентифікаційними даними і т. п. Додаткові відомості про фішинг-аферах і про захист від шахрайства в Інтернеті.

Регулярно змінюйте паролі. Це допоможе ввести зловмисників в оману. Чим надійніше пароль, тим довше можна його використовувати.

Пароль з 8 знаків-менш можна застосовувати протягом тижня, у той час як поєднання з 14 і більше знаків може служити кілька років, якщо воно складено за всіма правилами, наведеними вище.

Не вводьте паролі на чужих комп'ютерах. Комп'ютери в інтернет-кафе і лабораторіях, системи загального доступу, інтерактивні термінали, а також комп'ютери на конференціях і в залах очікування аеропортів не можуть вважатися безпечними і підходять тільки анонімного виходу в Інтернет. Не користуйтеся такими комп'ютерами для перевірки електронної пошти, банківського рахунку, доступу в віртуальні кімнати для розмов і доступу до інших облікових записів, де запитується ім'я користувача та пароль. Зловмисники застосовують недорогі і швидко встановлюються пристрої, що записують послідовність натиснень на клавіші. Такі пристрої дозволяють шахраям отримувати через Інтернет всі дані, введені в комп'ютер. Пам'ятайте, що ваші паролі і парольні фрази так само важливі, як і дані, які вони захищають.

Дії у разі викрадення пароля

Відстежуйте всі дані, захищені паролями: фінансові звіти за місяць, звіти про кредитні операції, дані про покупки через Інтернет і т. д. Надійні, легко запам'ятовуються паролі допомагають захиститися від шахрайства і розкрадання ідентифікаційних даних, але не є абсолютною гарантією захисту. Незалежно від того, наскільки надійним є пароль, якщо шахраям вдасться зламати систему, де він зберігається, вони його дізнаються. Якщо ви помітили підозрілі дії, які можуть означати, що хтось отримав доступ до ваших даних, як можна швидше повідомте про це у відповідні органи. Додаткові відомості про діях в разі викрадення ідентифікаційних даних або подібного шахрайства.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається паролем?
2. Яке програмне забезпечення називається менеджером паролів?
3. На які категорії діляться менеджери паролів.
4. Який принцип роботи менеджерів паролів?
5. Що називається онлайн менеджером паролів?
6. Назвіть основні переваги та недоліки онлайн менеджерів паролів.
7. Що являють собою менеджери паролів з бар’єрним захистом?
8. Назвіть правила створення та користування паролями.
9. Назвіть етапи створення надійного паролю.
10. Які програми управління паролями ви знаєте? Опишіть їх основні можливості.