УДК 004.056

Ю.В. Борсуковський, В.Л. Бурячок, П.М. Складанний

АНАЛІЗ СУЧАСНИХ ВИМОГ ДО СТВОРЕННЯ ПАРОЛЬНИХ ПОЛІТИК КОРПОРАТИВНИХ КОРИСТУВАЧІВ

В даній статті проведено детальний аналіз парольних політик. Сформульовані базові вимоги та рекомендації щодо створення парольних політик корпоративних користувачів з врахуванням останніх рекомендацій Національного Інституту Стандартів і Технології США.

Ключові слова: політика, стандарти, кібербезпека, автентифікація, авторизація, управління доступом.

Вступ і постановка задачі

До 2020 року світова економіка накопичувальним підсумком втратить від комп'ютерної злочинності $ 3 трлн, підрахували в компанії Microsoft. Прямі втрати всіх компаній світу через кібератаки досягли $ 400 млрд на рік. Такі дані навів заступник головного юриста Microsoft Джин Бёрс 13 жовтня 2016 на конференції з кібербезпеки CyberCrimeCon. До 2020 року сумарний збиток накопичувальним підсумком досягне $ 3 трлн. За словами Бёрса, щорічно жертвами кіберзлочинців стають більше 550 млн людей. 71% опитаних Microsoft компаній визнали, що були жертвами успішних IT-атак.

Цього року масштаб скомпрометованих облікових даних дійсно вражає: Dropbox (68 мільйонів акаунтів), LinkedIn (167 мільйонів), MySpace (360 мільйонів), Tumblr (65 мільйонів), Last.fm (43 мільйони), ВК (170 мільйонів). І один із елементів такої масштабної компрометації є пароль, що в незмінному вигляді багаторазово використовується користувачами у зв’язці адреси електронної пошти та пароля.

Враховуючи величезну кількість веб-сайтів і онлайн-додатків, що вимагають заводити все нові і нові облікові записи, користувачі обирають паролі доступу до них поспіхом, ігноруючи поради фахівців з безпеки.

Оскільки більш-менш прийнятної альтернативи в найближчій перспективі не існує, то відмовитися від паролів користувачам мабуть не вдасться. Статистика аналітичної компанії SplashData [4] ось уже який рік поспіль підтверджує цю думку.

Експерти SplashData щорічно аналізують мільйони вкрадених паролів в Інтернет-мережі і складають список з 25 найбільш популярних з них. Цього року такий список був складений на базі 2 мільйонів проаналізованих даних, що дозволило зробити висновок про те, що більшість користувачів й досі не розуміє важливості створення складного пароля, а не варіантів «123456» і «password» (що займають в цьому списку перші місця, таблиця 1), який є однією з основних складових якісної безпеки збереженої на комп'ютерах або в Інтернет-мережі інформації.

Таблиця 1

Список 25 найгірших паролів за 2015 рік

123456	123456789	Welcome	Dragon	Princess
Password	Football	1234567890	Master	Qwertyuiop
12345678	1234	abc123	Monkey	Solo
Qwerty	1234567	111111	Letmein	passw0rd
12345	Baseball	1qaz2wsx	Login	starwars

У зв'язку з цим Національний Інститут Стандартів і Технології (NIST) США сформулював нові рекомендації щодо створення парольних політик корпоративних користувачів [1]. В них вперше запропоновано використовувати шаблон для парольних політик організацій і програм розробки додатків з врахуванням «менталітету» користувачів та відмовитись від хибної практики виконання дій, що не поліпшують безпеку.

В умовах України з врахуванням вище зазначеного **актуальною** постає проблема коректного та найголовніше ефективного використання політик паролів, як для простих користувачів так і для користувачів, робота яких тісно пов’язана з комерційною або державною таємницею, вирішення якої можливе за рахунок адаптації рекомендацій NIST в політиках безпеки державного та приватного сектору [5,6].

Виклад основного матеріалу дослідження

Зважаючи на рекомендації, які висунув NIST, варто виокремити декілька основних тверджень.

Твердження 1.

Аутентифікація за допомогою відповідей на питання, які користувач дав заздалегідь, а також використання SMS-повідомлень в двофакторній аутентифікації через проблеми з безпекою їх доставки є неефективною. Це ґрунтується на тому, що:

- пристрій може бути заражений шкідливим програмним забезпеченням (ПЗ);
- можливе перенаправлення повідомлення зловмисникам;
- хакери можуть атакувати мережу оператора зв'язку та ін.

Твердження 2.

Встановлення терміну закінчення дії пароля без особливої необхідності є недоцільним (хоча практичний досвід дає підстави діяти навпаки - встановлювати термін життя складного паролю від 6 до 12 місяців).

Твердження 3.

Облікові дані доцільно змінювати тільки в разі, якщо вони були забуті, викрадені за допомогою фішингу або зламані.

Твердження 4.

Довжина пароля повинна бути не менше 8 та не більше 64 символів. При цьому доцільно використовувати парольні фрази та перевіряти паролі за допомогою частотних словників, а також відмовитись від хибної практики використання підказок та допоміжних питань, які спрощують злом паролів та їх відновлення (типу «В якій школі ви навчалися?», «Яке дівоче ім’я вашої матері?» і т.п.). Останнє твердження має велику цінність, оскільки паролі повинні зберігатися в хешованому вигляді з додаванням модифікатору (не менше 32 бітів), а обмеження довжини не повинно бути обов'язковим (модифікатор - рядок даних, яка передається хеш-функції разом з паролем. Використовується для подовження рядка пароля, щоб збільшити складність злому) [2]. При цьому користувачам додатково повинна бути забезпечена можливість використовувати всі друковані символи ASCII, пробіли та символи UNICODE, включаючи емодзі (смайлики). Використання парольних фраз та їх перевірка за допомогою частотних словників дозволить вибирати будь-які існуючі знаки пунктуації та будь-яку вибрану користувачами мову, а також виключити з вжитку такі широко вживані варіанти, як «qwerty» та «ThisIsPassword» і т. д.

На підставі аналізу вищевикладених рекомендацій NIST, варто сформулювати базові вимоги щодо створення парольних політик корпоративних користувачів (табл.2). Для зручності приведемо їх у вигляді правил, що легко можуть бути адаптовані в будь яку парольну політику. Нагадаємо, що парольна політика встановлює вимоги до порядку вибору, зберігання, використання, періодичності зміни і інших питань, пов'язаних із застосуванням механізмів парольної аутентифікації в інформаційних системах та прикладних додатках.

Таблиця 2

Вимоги щодо створення парольних політик корпоративних користувачів

№ правила	Формулювання вимоги
Правило 1.	Довжина пароля повинна становити понад 8 символів. При цьому пароль має бути схожим більше на криптографічний ключ у вигляді набору випадкових символів, ніж на секретне слово. Так, наприклад: при довжині пароля від 8 до 11 символів обов'язково повинен використовуватися мікс (суміш) букв на нижньому і верхньому регістрі, цифр і спецсимволів [3]; довжина пароля від 12 до 16 символів має передбачати використання міксу букв на нижньому і верхньому регістрі та цифр; довжина пароля від 16 до 21 символу має ґрунтуватися на використанні міксу букв на нижньому і верхньому регістрах; при довжині пароля понад 22 символи доцільно використовувати будь-які літерні символи. Довжина пароля для мобільних пристроїв не повинна бути менше 15 символів. Вміст пароля має складатися з букв і цифр нижнього і верхнього регістрів. Наприклад: пароль для банківського додатку: 8xaFTMT8OZWxa1xv.
Правило 2.	Пароль не може складатися з одного слова, яке з'являється в словнику (українською або будь якою іншою мовою). При формуванні пароля доцільно використовувати парольні фрази з кількох слів. *Примітка*: не всі сайти і додатки підтримують таку можливість. Часто довжина пароля обмежується зверху, що не дозволяє використовувати при формуванні пароля довгі фрази.
Правило 3.	У стійкому паролі повинно бути не менше 3-х спецсимволів, 3-х цифр, 3-х заголовних і 3-х малих літер. Для легкого запам'ятовування користувачем вимог до побудови пароля – назвемо це правило «правилом 3х4». Приклад побудови стійкого паролю: ФРАЗА: «Їжачок в тумані. Мультфільм хороший та веселий» ПАРОЛЬ: - ***v~DisneyGo0d:)** • "*" - «їжачок»; • "v" - «в»; • "~" - «туман»; • "Disney" - популярна студія мультфільмів; • "Go0d" - "good" –> «золото» -> «хороший»; • ":)" - «веселий». ФРАЗА: «Сніг взимку, а влітку сонце» ПАРОЛЬ: - ***Dpbvre@Dksnre/o** • "*" - «сніг»; • "Pbvjq" - на англійській розкладці українськими буквами «Взимку»; • "@" - «а»; • "Ktnjv" - на англійській розкладці українськими буквами «Влітку»; • "/o\" - «сонце». *Примітка*: не використовуйте жоден з наведених прикладів в якості пароля!

Правило 4.	При великій кількості облікових записів (більше трьох) бажано використовувати функціонал менеджеру паролів та запровадити додатковий захист бази даних і ключового файлу користувача за допомогою сертифікату. Для цього може бути застосований будь-який зовнішній носій з апаратним шифруванням (на кшталт eToken), використання якого дозволить користувачеві зберігати сертифікати, секретні ключі та бази даних менеджера паролів. Політика блокування облікових записів користувачів повинна бути при цьому орієнтована на такі вимоги: • кількість помилкових вводів пароля – хх (рекомендується 11); • час блокування облікового запису - хх год (рекомендується 3 год.); • час доступу користувачів до Active Directory - з хх.хх до хх.хх.
Правило 5.	З метою запобігання несанкціонованого доступу до робочих місць користувачів, а також до ресурсів корпоративної мережі з використанням чужих облікових записів (імен користувачів), користувачі зобов'язані блокувати екрани своїх комп'ютерів в разі залишення ними свого робочого місця натисканням на комп'ютерній клавіатурі набору клавіш Ctrl + Alt + Del і далі - кнопки «Блокування» («Lock Workstation»).
Правило 6.	Користувачам ***<u>забороняється</u>***: • повідомляти свій пароль кому-небудь, включаючи колег, керівників і фахівців служби технічної підтримки; • зберігати паролі в доступній для сприйняття формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, функціональних клавішах терміналу, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де неуповноважені особи можуть отримати до них доступ; • записувати паролі і залишати ці записи в місцях, де до них можуть отримати доступ неуповноважені особи; • використовувати загальні паролі для доступу до інформаційних систем та інтернет-ресурсів будинку і на робочому місці; • використовувати загальні паролі спільно з іншими співробітниками організації.

Користувачі, що порушують вимоги цієї політики, можуть бути піддані дисциплінарним стягненням, включаючи догану та звільнення з роботи за грубе порушення правил роботи в корпоративній мережі.

Висновок

Питання організації безпеки користувачів, а зокрема інформації яку користувачі передають, на даний час досить гостро стоїть у цілому світі. Проаналізовані і сформовані рекомендації для використання парольних політик організації різних форм власності, можуть допомогти суттєво зменшити ризики пов’язані з несанкціонованим доступом до інформації, втратою інформаційних ресурсів, компрометації організації і т.п. Подальші дослідження варто зосередити на створенні та впровадженні типової політики для використання даних правил і рекомендацій та навчанні персоналу.

Література:

1. Digital Authentication Guidelines. Special Publication 800-63-3: NIST; 2016
2. Бернет С., Пэйн С. Криптографія. Офіційне керівництво RSA Security: БІНОМ; М.; 2002
3. Стенфордський університет. Служба IT університету (https://uit.stanford.edu); 2016
4. SplashData. SplashID password manager (http://splashdata.com), 2016
5. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.
6. Бурячок В.Л. Політика інформаційної безпеки: навчальний посібник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 134 с

Надійшла 08.08.2016 р. Рецензент: д.т.н., проф. Горбенко І. Д.