Шаблонність людського мислення та комп'ютерна безпека

Заболоцький П.В., студент навчальної групи 22-ПС факультету №2 НАВС

Науковий керівник:доцент кафедри інформаційних технологій ННІ №1 Національної академії внутрішніх справ **Пакриш О.Є.**

В останні роки інформаційні технології розвиваються найбільш активно, а разом із цим відбуваються розробки в сфері інформаційної безпеки та впровадження більш високий стандартів. Засоби шифрування інформації стають все більш складними, але це не заважає зловмиснику скористатися можливістю отримати дані користувача, а все через те, що людський фактор все ще відіграє велику роль, а саме – шаблонність мислення.

Для початку зазначимо, що таке мислення. Мислення – це система свідомих операцій спрямованих на розв'язання задач за допомогою розкриття властивостей об'єкта, тобто для знаходження відповіді на певне питання необхідно провести низку операцій, якість і швидкість виконання яких залежить від здібностей людини. Для того, щоб зберегти час та сили людина починає використовувати шаблони, тобто раніше знайдені відповіді, що підходять за запитом. Отже, шаблонне мислення – це такий спосіб мислення, під час якого не відбувається створення чогось нового, а використовуються раніше створені відповіді, що підходять до певних умов.

Гарним прикладом шаблонного мислення є пароль користувача. На будь-якому сайті, де зберігається інформація користувача, завжди дають рекомендації щодо безпечного паролю, але частіше всього користувачу не хочеться вигадувати складний пароль. Таке зустрічається не тільки серед звичайних користувачів, але й серед системних адміністраторів. За інформацією дослідницької компанії Trustwave, більше чверті інцидентів, пов'язаних з безпекою, відбулися через те, що системний адміністратор використовував слабкий пароль. Trustwave проаналізували 574 випадки, серед яких 28% несанкціонованого доступу були через небезпечні паролі.

Інша дослідницька компанія WP Engine проаналізували 10 млн. скомпрометованих паролів, що використовувалися від студентів до генеральних директорів. Виявилося, що найпопулярніші паролі це звичайні слова та комбінації. Наприклад 123456; password; 12345678; qwerty; 12345; 1234 і т.д. Тут з'являється особливість шаблонного мислення, що описувалася раніше – люди в цьому випадку думають не про власну безпеку, а про те, з якою швидкістю вони будуть відтворювати пароль. WP Engine також виявили, що одним з найпопулярніших слів у паролі є слово love. Окремо чи в комбінаціях це слово зустрілося 40 тис., особливо у користувачів жіночої статі в комбінаціях ilove[ім'я].

Шаблони це не є погано, це звичайне та притаманне людині прагнення полегшити своє життя, але на вище зазначених прикладах можна побачити як шаблони навпаки ускладнюють життя через втрачену інформацію, бо пароль був шаблонний. Щодо власної безпеки ніколи не варто бути легковажним, тому далі будуть представлені правила створення паролю та безпечне користування в інформаційною сферою:

1. Довжина паролю повинна бути більше 10 символів. Пароль з 8 символів можна дізнатися за один день, а з 10 – декілька місяців.
2. Пароль повинен мати літери різного регістру, цифри, символи.
3. Не використовувати власні імена, прізвища, дати народження як паролі.
4. Не використовувати один і той самий пароль в різних системам, бо якщо вас зламають, то зловмисник матиме доступ до всієї вашої інформації.
5. Не зберігати паролі в браузері, за допомогою функції «зв'язка ключів».
6. Намагатися не використовувати загальнодоступні WI-FI мережі.
7. Використовувати подвійну аутентифікацію.

Правила не дуже складні, але вони збережуть вашу інформацію, а тому і нервову систему.