Дослідження випадків несанкціонованого доступу до урядових інформаційних ресурсів

Ігор Дмитрусь, Дмитро Тарасов

Кафедра соціальних комунікацій та інформаційної діяльності, Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С. Бандери, 12, E-mail: igorkositin@gmail.com

Abstract – In the paper investigated government sites for unauthorized access. Statistics showed number of unauthorized access during the period 2012-2013.

Ключові слова – інформаційний ресурс, сайт, несанкціонований доступ, злом.

Недосконалі засоби захисту інформаційних ресурсів підвищують імовірність злому, що призводить до крадіжки або публічного розповсюдження конфіденційної інформації. Для уникнення подібних ситуацій потрібно наймати спеціалістів та здійснювати кваліфіковане обслуговування сайту.

У статті викладені результати дослідження, в якому проводився аналіз випадків вторгнень у сайт за період 2011–2013 рр. Можна зробити наступні висновки: всього за 2012 р. було зломано 147 урядових сайтів, за 2013 р. таких випадків зареєстровано 140 сайтів. Зазначимо методи злому інформаційного ресурсу: заміна головної сторінки сайту на сторінку зловмисника, заміна однієї із сторінок сайту на іншу, створення або заміна зображень сайту, заміна документів.

Статистичні дані кількості випадків злому за досліджуваний період показують, що за 2012 р. кількість випадків заміни головної сторінки сайту 105, крім цього заміна сторінок ресурсу – 21 випадок, підміна документів ресурсу – 2 випадка; за 2013 кількість випадків заміни головної сторінки сайту 53, заміна сторінок ресурсу – 49 випадок, підміна документів ресурсу – 24 випадка, підміна зображень – 8 випадків. Декілька інформаційних ресурсів було повторно зломано: у 2012 р. – 17 випадків, у 2013 р. – 41.

Загальна кількість зломів за 2012р. становить 145 випадків, за 2013р. – 181 випадок. Простежується тенденція зростання кількості зловмисних дій над урядовими інформаційними ресурсами і вже за січень-лютий 2014 р. було зафіксовано 22 випадки.

Із загальної кількості сайтів, що піддалися впливу зловмисних дій у 2012 р. 45 належать районним державним адміністраціям, 11 – державним підприємствам, 7 – міським радам, 6 – науковим установам, 5 – Кабінетам Міністрів, 6 – інвестиційним порталам, 4 – обласним державним адміністраціям, 3 – Департаментам соціального захисту, 2 – пенсійним фондам, 1 – державним агентствам, 1 – центру зайнятості.

За 2013 р. зафіксовано 32 зломи сайтів районних державних адміністрацій, зросла кількість зломів сайтів державних агентств (агентства земельних

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

ресурсів, водних ресурсів лісових та ін.) порівняно з попереднім роком – 13 випадків посягань, державних підприємств – 9 випадків, наукових установ – 8, управлінь внутрішніх справ – 5, міських рад – 4 випадки, обласних державних адміністрацій – 4, інвестиційних порталів – 2 випадки, Кабінету Міністрів України – 1 зловмисний випадок та 1 випадок злому сайту центру зайнятості.

Отже, найбільш популярними за кількістю посягань зловмисників є сайти державних районних адміністрацій, державних підприємств, державних агентств, наукових установ. Найбільшою популярністю на посягання зловмисниками користуються ресурси, які містять інформацію, що є власністю держави або інформацію з обмеженим доступом серед випадків несанкціонованих дій чи порушень цілісності інформації з метою заволодіння (для власного користування або для подальшого продажу) чи одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду).

Основними критеріями, за якими можна характеризувати сайт є актуальність та достовірність інформації. Складність оцінювання сайту на достовірність інформації полягає насамперед в тому, що не існує одного конкретного критерію (ознаки чи фіксованої сукупності ознак), за яким можна було б оцінити сайт, як достовірний, натомість, актуальність інформації перевірити можливо.

Статистика оцінювання інформації сайту на актуальність демонструє, що на сьогоднішній день із сайтів, які були досліджені, систематично оновлюють інформацію 177, кількість сайтів, які працюють але не оновлюють інформацію – 126, сайтів, які припинили свою роботу після зловмисних дій є 109. Важливими критеріями безпеки інформаційних ресурсів є технічне забезпечення, яке використовується. Серед досліджених інформаційних систем (400 інформаційних ресурсів) близько 24% наповнені, використовуючи CMS Joomla, 2% – CMS Drupal, CMS WordPress використовували 3% розробників. Статистика показує, що робота інформаційних ресурсів базується на використанні інформаційних систем, серед яких 70% Linux, 25% FreeBSD та 3%Windows 2003.

Варто зазначити, що після злому урядових сайтів, зловмисники залишають після себе авторський підпис, проаналізувавши який можна з'ясувати країну та групу зловмисників. З'ясувалося, що найбільше випадків зловмисних дій було здійснено із Індонезії – 30%, Бразилії – 24%, Туреччини – 14%, Алжиру – 11%, Сирії – 7% та Афганістану – 5%.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua