УДК 004.056
DOI: 10.25140/2411-5363-2020-2(20)-237-240

Сергій Семендяй, Михайло Шелест, Юлія Ткач, Леся Черниш

ЕТИЧНИЙ ХАКІНГ У БІЗНЕС-КОМПАНІЯХ ТА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ

Актуальність теми досліджень. *Бурхливий розвиток IT-технологій та інтенсивна інформатизація усіх сфер суспільства веде до появи нових інформаційних загроз, тому інформаційна безпека є одним із найбільш важливих завдань IT-індустрії. Важливим елементом у процесі розробки нових методів захисту інформації є пошук вразливостей інформаційних систем.*

Постановка проблеми. *Перспективним напрямом у галузі захисту інформації є розробка активних методів забезпечення захисту, з-поміж яких можна виділити пошук вразливостей інформаційних систем.*

Аналіз останніх дослідженнь і публікацій. *У сучасних дослідженнях інформаційної безпеки значне місце посідають етичний хакінг та проведення тестів на проникнення, залишаючи в тіні такий дієвий засіб, як дослідження волонтерами вразливостей державних інформаційних ресурсів.*

Виділення недосліджених частин загальної проблеми. *Нині в роботах вітчизняних та закордонних учених недостатньо уваги приділяється можливостям дослідження волонтерами вразливостей державних інформаційних ресурсів.*

Постановка завдання. *Мета статті полягає у висвітленні різниці між підходами до забезпечення кібербезпеки в бізнес-структурах та державних органах України.*

Виклад основного матеріалу. *Клієнти надають IT-компаніям дедалі більше особистої інформації, а компанії повинні її оберігати. Але практично в кожній програмі є вразливості, отже, персональні дані клієнтів можуть опинитися у руках злочинців.*

Висновки відповідно до статті. *Показником роботи кіберполіції є розкриття злочинів. Так, кіберполіція робить багато корисного, наприклад, ловить шахраїв і розповсюджувачів дитячого порно. Однак специфічних комп'ютерних злочинів розкрито одиниці. Тобто рівень захисту з боку держави як власних ресурсів, так і громадян від злочинних посягань поки що низький.*

Ключові слова: *етичний хакінг; комп'ютерні мережі; кібербезпека; захист інформації; виявлення вразливостей. Бібл.: 2.*

Актуальність теми дослідження. Бурхливий розвиток IT-технологій та інтенсивна інформатизація всіх сфер суспільства веде до появи нових інформаційних загроз, тому інформаційна безпека є однією з найбільш важливих задач IT-індустрії. Важливим елементом в процесі розробки нових методів захисту інформації є пошук вразливостей інформаційних систем.

Постановка проблеми. Компаніям доводиться керуватись принципом «хочеш протистояти хакерам – думай, як хакер». Бізнес активно залучає до співпраці етичних хакерів, котрі шукають помилки та допомагають їх виправити раніше, ніж про вразливість стане відомо хакерам-зловмисникам. Проте державні установи майже зовсім не використовують такий інструмент, як етичний хакінг.

Аналіз останніх досліджень та публікацій. У сучасних дослідженнях інформаційної безпеки значне місце посідають етичний хакінг та проведення тестів на проникнення, залишаючи в тіні такий дієвий засіб, як дослідження волонтерами вразливостей державних інформаційних ресурсів.

Виділення недосліджених частин загальної проблеми. На сьогодні в роботах вітчизняних та зарубіжних вчених недостатньо уваги приділяється можливостям дослідження волонтерами вразливостей державних інформаційних ресурсів.

Мета статті. Головною метою цієї роботи є огляд та аналіз різних підходів до забезпечення кібербезпеки в бізнес-структурах та державних органах України.

Виклад основного матеріалу. Клієнти надають IT-компаніям дедалі більше особистої інформації, а компанії повинні її оберігати. Але практично в кожній програмі є вразливості, отже, персональні дані клієнтів можуть опинитися в руках злочинців.

Хакери займаються пошуком таких вразливостей – багів (небезпечних помилок) у програмах, вебсервісах чи мобільних застосунках. Хакери-злочинці продають свої знахідки на чорному ринку, використовують для шантажу чи самоствердження, псуючи чужі IT-продукти.

Етичні хакери діють відкрито, за визначеними правилами, і передають інформацію про знайдені вразливості компаніям, щоб ті виправили помилки. Зазвичай компанія виплачує за це грошову винагороду. Таку співпрацю називають «bug bounty» (винагорода за баг), а шукачів вразливостей – «баг-хантерами».

Історія етичного хакінгу починається у 70-х роках XX сторіччя. Одними з перших такий підхід почали використовувати військово-повітряні сили США. На комерційні рейки етичний хакінг став у 1995 році, коли було відкрито першу у світі bug bounty програму в компанії Netscape.

Бізнес або самостійно організовує програму bug bounty (як Facebook чи Google), або ж відкриває програму на спеціальній платформі, де зареєстровані тисячі етичних хакерів з усього світу.

У світі існує десяток активних bug bounty платформ, одна з яких – українська HackenProof. Принцип роботи платформ простий. Компанія розміщує інформацію про свою програму: які компоненти системи треба перевірити, яка винагорода передбачена.

Етичний хакер повинен дотримуватись правил і досліджувати лише дозволені ділянки. Коли він знаходить баг, то надсилає звіт: описує процес злому й поради щодо виправлення.

Звіт перевіряє спеціальна команда інженерів, і якщо вразливість підтверджується, баг-хантеру виплачують винагороду. Кожен баг має свій «рівень». Найбільше платять за критичні вразливості – ті, що дозволяють отримати доступ адміністратора і вносити будь-які зміни в систему.

Також розмір винагороди залежить від конкретної компанії. Наприклад, одному учаснику ком'юніті корпоративний месенджер Slack заплатив за критичну вразливість 1000 $, Uber за такий же небезпечний баг —3000 $.

Баг-хантери зазвичай зареєстровані одразу на кількох платформах, де шукають цікаві для себе задачі. Учасники з високим рейтингом мають доступ до закритих програм. Також етичні хакери періодично їздять на профільні заходи, де змагаються в пошуку вразливостей та діляться знаннями.

Часто у етичного хакера є конкретна спеціалізація та кілька коронних технік. Хтось спеціалізується на вебсервісах, хтось – на блокчейн-проєктах і криптовалютах, хтось – на мобільних застосунках.

Навесні 2016 року виникла спільнота українських кіберактивістів з різних міст України і куточків світу – Український кіберальянс (УКА, англ. Ukrainian Cyber Alliance, UCA). Український кіберальянс ексклюзивно передає добуті дані для аналізу, дорозвідки та оприлюднення міжнародній розвідувальній спільноті ІнформНапалм, а також силовим структурам України.

Відповідальне розголошення (responsible disclosure) – термін у кібербезпеці, який визначає, що вразливості, знайдені в системі, деякий час не виходять назовні, щоб її власники встигли їх виправити. Українські хактивісти довгий час намагались працювати саме так, сподіваючись, що чиновники почнуть більш відповідально відноситись до роботи, але не дочекались цього. У результаті Український кіберальянс провів серію перевірок під лозунгом #FuckResponsibleDisclosure, публікуючи знайдені недоліки. З-поміж тих, у кого є проблеми з кібербезпекою, – Центр космічного зв'язку, Запорізька АЕС, військкомати та багато інших держустанов. Відкриті для всього Інтернету системні диски із закритою інформацією, прості паролі до системних акаунтів, а то й узагалі їх відсутність – ось лише незначна частина знахідок, які хактивісти опублікували у Facebook під згаданим вище хештегом.

Наслідки, до яких могли призвести ці дірки в захисті інформації, найрізноманітніші – від витоку даних про бійців АТО до дистанційного управління регіональними водоканалами. За думкою хактивістів, писати відповідальним за це особам марно. У найкращому

разі вони закриють тихенько дірку й на тому все закінчиться. Тобто це означає, що інші про атаку нічого не знатимуть і не зможуть підготуватися. А коли державні організації присоромлюють публічно, то це таки дає певний ефект.

З-поміж знайдених ресурсів фігурують Управління національної поліції в Києві, Академія МВС – на відкритому диску лежала база даних сайтів і база офіцерів, НАЗК, «Енергоатом», включно з відділом ядерної безпеки Запорізької АЕС – у них у відкритому доступі лежало все, починаючи від креслень реактора 1984 року й до останніх звітів. У Кіровоградському водоканалі відкритою виявилась система віддаленого керування водопроводом, у Рівненському – доступ до локальної мережі.

Херсонська обласна рада залишила в у відкритому доступі загальний диск з документами. Одне з київських комунальних підприємств виклало онлайн свою бухгалтерію й ключ від розрахункового рахунку. Були виявлені витоки документів мобільних операторів "Київстар" і Vodafone — служби безпеки операторів почали реагувати через лічені секунди після публікації. У випадку із сайтами РНБО й Конституційної комісії при президентові України реакція послідувала беззастережно, їм знадобилось від доби до тижня щоб закрити або виправити скомпрометовані ресурси.

Висновки відповідно до статті. Показником роботи кіберполіції є розкриття злочинів. Так, кіберполіція робить багато корисного, наприклад ловить шахраїв і розповсюджувачів дитячого порно. Однак специфічних комп'ютерних злочинів розкрито одиниці. Тобто рівень захисту з боку держави як власних ресурсів, так і громадян від злочинних посягань поки що низький. За думкою фахівців з Українського кіберальянсу, вимоги до обслуговування державних ресурсів такі, що протирічать самі собі й не можуть бути виконані. Необхідно спростити законодавство, скоротити зайві організації, звільняти людей, що не справляються з поставленими завданнями. Ускладнення законів, надії на чудодійні закордонні залізяки або запрошених чудо-спеціалистів – це шлях у нікуди. В Україні відкрито кіберцентри, які посилено займаються освоєнням бюджетів і грантів, але результатів їх роботи не видно.Тому, якщо немає грошей на те, щоб зробити все заново на більш високому рівні, можна спростити наявну систему. Треба донести до виконавців просту думку, що информація – це цінність, її необхідно захищати. Треба визнати наявність проблеми й обговорити її публічно, а не займатися перекладанням відповідальності.

Список використаних джерел

1. Піскозуб А. З. Використання вільного програмного забезпечення для підвищення рівня захищеності комп'ютерних мереж та систем. *Матеріали другої міжнародної науково-практичної конференції FOSS Lviv 2012*. Львів, 2012. С. 86-90.

2. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements 3. Shakeel Ali, Tedi Heriyanto. BackTrack 4: Assuring Security by Penetration Testing. Master the art of penetration testing with BackTrack. *Packt Publishing Ltd*. Birmingham, 2011. 373 p. 4. URL: http://www.kali.org.

References

1. Piskozub, A. Z. (2012). Vykorystannia vilnoho prohramnoho zabezpechennia dlia pidvyshchennia rivnia zakhyshchenosti kompiuternykh merezh ta system [The use of free software to increase the level of security of computer networks and systems]. *Materialy druhoi mizhnarodnoi naukovo-praktychnoi konferentsii FOSS Lviv 2012 – Proceedings of the second international scientific-practical conference FOSS Lviv 2012* (pp. 86-90). Lviv [in Ukrainian].

2. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements 3. Shakeel Ali, Tedi Heriyanto. BackTrack 4: Assuring Security by Penetration Testing. Master the art of penetration testing with BackTrack (2011). *Packt Publishing Ltd*. Birmingham. Retrieved from http://www.kali.org.

UDC 004.056

Serhii Semendiai, Mykhaylo Shelest, Yuliia Tkach, Lesya Chernysh

ETHICAL HACKING IN BUSINESS COMPANIES AND DETECTION OF VULNERABILITIES IN INFORMATION SYSTEMS OF STATE AUTHORITIES OF UKRAINE

Urgency of the research. *The rapid development of IT technologies and intensive informatization of all spheres of society leads to the emergence of new information threats, so information security is one of the most important tasks of the IT industry. An important element in the development of new methods of information protection is the search for vulnerabilities in information systems.*

Target setting *A promising area in the field of information security is the development of active methods of providing protection, among which we can highlight the search for vulnerabilities of information systems.*

Actual scientific researches and issues analysis. *Ethical hacking and penetration testing play a significant role in modern information security research, leaving in the shadows such an effective tool as volunteer research into the vulnerabilities of public information resources.*

Uninvestigated parts of general matters defining. *Currently, in the works of domestic and foreign scientists, insufficient attention is paid to the opportunities for volunteers to study the vulnerabilities of state information resources.*

The research objective. *The purpose of the article is to highlight the differences between approaches to cybersecurity in business structures and government agencies of Ukraine.*

The statement of basic materials. *Customers are providing more and more personal information to IT companies, and companies need to protect it. But virtually every program has vulnerabilities, so personal customer data can end up in the hands of criminals.*

Conclusions. *An indicator of the work of cyberpolice is the detection of crimes. Yes, cyberpolice does a lot of good, such as catching fraudsters and distributors of child porn. However, specific computer crimes have been uncovered. That is, the level of protection by the state of both its own resources and citizens from criminal encroachments is still low.*

Keywords: *ethical hacking; computer networks; cybersecurity; information security; vulnerability detection.*

References: 2.

Семендяй Сергій Матвійович – завідувач лабораторії кібербезпеки, аспірант, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Semendiai Serhii – Head of the cybersecurity laboratory, PhD Student, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: sovnarcom@ukr.net
ORCID: http://orcid.org/0000-0002-7751-5956

Шелест Михайло Євгенович – доктор технічних наук, професор, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Shelest Mykhailo – Doctor of Technical Science, Professor, Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mishel3141@gmail.com
ORCID: https://orcid.org/0000-0003-1090-0371
SCOPUS Author ID: 57211429755

Ткач Юлія Миколаївна – доктор педагогічних наук, доцент, завкафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна)
Tkach Yuliia – Doctor of Pedagogical Science, Associate Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: https://orcid.org/0000-0002-8565-0525
SCOPUS Author ID: 57193026076

Черниш Леся Григоріївна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, , Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: lg4@ukr.net
ORCID: http://orcid.org/0000-0001-7446-1684

Семендяй С., Шелест М., Ткач Ю., Черниш Л. Етичний хакінг в бізнес-компаніях та виявлення вразливостей в інформаційних системах державних органів України. *Технічні науки та технології.* 2020. № 2 (20). С. 237-240.