Борумбєй Богдан Ігорович
Національний університет «Одеська юридична академія»,
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

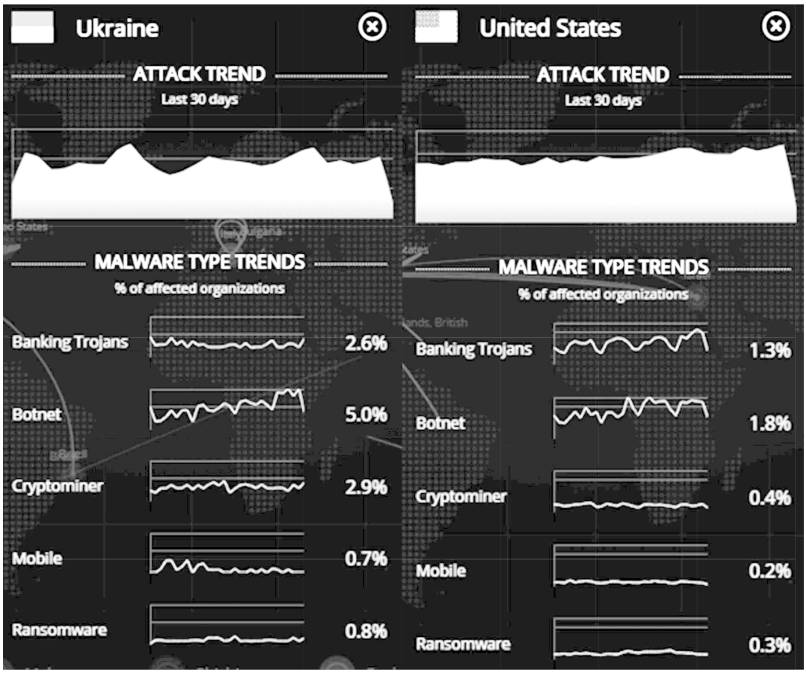
Борумбєй Тетяна Ігорівна
Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ПРОБЛЕМЫ КИБЕРПРОСТРАНСТВА В УКРАИНЕ

Термин «диджитализация» начали употреблять еще в 2019 году. Он означает автоматизацию всех бытовых процессов, используя интернет-технологии. С каждым днем появляются новые идеи, разрабатываются платформы, которые автоматизируют процессы, требовавшие к себе особого внимания. Сейчас достаточно зайти на определенную платформу и решить возникшую проблему за считанные секунды. Но так ли все просто? Каждая из платформ требует от пользователя регистрации или даже верификации, соответственно данные пользователя сохраняются в базе данных для дальнейшей авторизации. Данные требуют некой конфиденциальности от вторых и в особенности от третьих лиц. Этому посвящен целый раздел в конвенции об обеспечении международной информационной безопасности. Но на сколько хороша информационная безопасность платформ, которые мы используем на территории Украины?

Анализируя статистику службы безопасности Украины можно сказать, что с начала 2020 года было заблокировано 2,5 тысячи веб-ресурсов, которые использовались в преступных целях, и деятельность 20 хакерских группировок [3]. Также СБУ нейтрализовала 460 киберинцидентов и кибератак на органы государственной власти и критически важные объекты инфраструктуры. [3] Не считая официально

зарегистрированные кибератаки, описанные выше инциденты можна умножить приблизительно в 2 раза. В первую очередь приведенные данные говорят о том, что информационная безопасность и киберпространство Украины, мало защищённые от кибератак. По статистике интерактивной карты киберугроз ThreatCloud World Cyber Threat Map, созданной компанией Check Point, за последний месяц Украина превосходи по количеству кибератак даже США (Схема 1). Система постоянно анализирует сайты в сети на наличие ботов, каждый день обнаруживая, в среднем, более миллиона типов вредоносных программ. Если учитывать то, что представленная платформа регистрирует явна не все кибератаки, данные показатели являются приблизительными и фактически могут быть увеличены в несколько раз.



(Схема 1) [1]

Проблемы уязвимости большинства платформ в частности на территории Украины связаны с отсутствием проверки на проникновение коммерческих проектов перед выгрузкой их в сеть. Многие компании очень часто отказываются привлекать к разработке «продукта» специалистов, что чревато для пользователей и в особенности для компаний, ведь в этом случае страдает экономическая составляющая компаний и качество разработки. Кроме этого уязвимостям способствует исходный код платформы и использование устаревших технологий в особенности в Украине, так как найти разработчика, который использует старые технологии, намного дешевле, чем нанимать квалифицированного специалиста.

Огромное количество процессов автоматизируется и можно только представить сколько конфиденциальной информации «сливается» в сеть. Поэтому внедрение таких обязательств как тестирование платформ на проникновение следует применять как обязательную составляющею информационной безопасности. Уязвимости киберпространства можно разделить на несколько видов:

1. Компьютерная неграмотность. Связана с большим количеством кибермошенников которые пользуются неграмотностью людей с целью получения от потенциальной цели информации или денежного вознаграждения. Как пример, к данной категории можно отнести интернет рассылки. Так для получения доступа к системе компании киберпреступнику достаточно сделать рассылку с вредоносной ссылкой или какой-либо вирусной программой на почты всех сотрудников, притворяясь, скажем, налоговой службой. Вероятность, что один из 100 сотрудников нажмет на эту ссылку, достаточно велика и киберпреступнику уже не составит труда получить желаемую информацию.

2. Присутствие популярных уязвимостей, включая:

• IDOR (Insecure Direct Object Reference, небезопасные прямые ссылки на объекты) – уязвимость, которая позволяет получить несанкционированный доступ к веб-страницам или

файлам. Самый распространенный случай IDOR – когда злоумышленник перебирает предсказуемый идентификатор и получает доступ к чужим данным.

• XSS – Cross Site Scripting (межсайтовое выполнение сценариев). Когда происходит XSS-атака, в веб-страницу встраивается вредоносный код. И как только посетитель сайта откроет эту страницу, начнёт выполняться какой-либо неприятный сценарий. Чаще всего под вредоносным кодом подразумевается внедрение html-тегов или скриптов на JavaScript.

• SQL-инъекция – это атака, направленная на сайт или веб-приложение, в ходе которой пользователь может обходным путём получить информацию из базы данных с помощью SQL-запросов. В случае успешной атаки пользовательские данные интерпретируются как часть SQL-кода запроса, и таким образом изменяется его логика.

Решение проблем, связанных с уязвимым киберпространством Украины можно решить, используя различные нововведения в нынешнею систему. В качестве распространения информации пользователи, развивая свои знания в сфере информационной безопасности и компьютерной грамотности, могут использовать средства массовой информации, узнавая про основы социальной инженерии, веб-угрозы, различные киберприступления такие как: кардинг, фишинг, методы шифрования информации и данных и т.д. Также можно поспособствовать полной переквалификации преподавательского состава всех высших учебных заведений для обеспечения качественного образования студентов и выпуска квалифицированных кадров. Еще одним решением проблемы уязвимости киберпространства является использование и внедрение новых технологий для разработки платформ. Важным аспектом для предотвращения похищения информации является введение неких «правил» в правовом поле. В Украине реализация информационной защиты с помощью законодательства находится на достаточно низком уровне. Именно данные решения поспособствуют и организуют максимальную безопасность киберпространства.

Подводя итоги, можно сказать, что на данном этапе так называемая «диджитализация» важный процесс, однако крайне незащищенный, ведь это не просто автоматизация привычных человеку действий. Для правильного использования информации защиты данных пользователю необходима защита на уровне закона, но кроме этого знание и понимание процессов, развитие компьютерной и медиаграмотности.

Список використаних джерел:

1. MAP. ThreatCloud World Cyber Threat Map [Електронний ресурс]. Режим доступу до ресурсу: https://threatmap.checkpoint.com/.

2. Артём Мышенков. Популярные уязвимости сайтов: чем опасны и как их избежать [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://cmsmagazine.ru/journal/items-popular-site-vulnerabilities/.

3. Кулеш С. Статистика: кількість кібератак за 2020 рік «СБУ: У 2020 році було нейтралізовано 20 хакерських угруповань і 460 кібератак на критично важливі об'єкти» [Електронний ресурс] / С. Кулеш. – 2020. – Режим доступу до ресурсу: https://itc.ua/news/sbu-v-2020-godu-bylo-nejtralizovano-20-hakerskih-gruppirovok-i-460-kiberatak-na-kriticheski-vazhnye-obekty/.

Ключові слова: уразливості кіберпростору, інформаційна безпека, кібернетична безпека, застарілі технології, уразливості, уразливості при веб-розробці, уразливості інформаційної безпеки, захист від вразливостей.

Ключевые слова: уязвимости киберпространства, информационная безопасность, кибернетическая безопасность, устаревшие технологии, уязвимости, уязвимости при веб-разработке, уязвимости информационной безопасности, защита от уязвимостей.

Keywords: cyberspace vulnerabilities, information security, cyber security, outdated technologies, vulnerabilities, vulnerabilities in web development, information security vulnerabilities, protection against vulnerabilities.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*