20 години катедра "Търговски бизнес"

Стопанска академия „Д. А. Ценов" - Свищов

Факултет „Производствен и търговски бизнес"
Катедра „Търговски бизнес"

Юбилейна научнопрактическа конференция
с международно участие

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС – КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

Том II

12-13 май 2011 г.

Свищов, 2011 г.

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ" СВИЩОВ
ФАКУЛТЕТ „ПРОИЗВОДСТВЕН И ТЪРГОВСКИ БИЗНЕС"
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

ЮБИЛЕЙНА НАУЧНОПРАКТИЧЕСКА КОНФЕРЕНЦИЯ
С МЕЖДУНАРОДНО УЧАСТИЕ

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

12-13 май 2011 г.

Том II

20 ГОДИНИ
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

Академично издателство „Ценов" Свищов
2011 г.

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Председател: Доц. д-р Марияна Божинова

Членове: Доц. д-р Петранка Мидова
Доц. д-р Светослав Илийчовски
Доц. д-р Симеонка Петрова
Доц. д-р Теодора Филипова
Доц. д-р Петя Иванова

Конференцията се посвещава
на 20-годишния юбилей
на катедра „Търговски бизнес"
и на 75-годишнината от създаването
на Стопанска академия „Д. А. Ценов"
Свищов.

Публикуваните доклади не са редактирани и коригирани. Авторите носят пълна отговорност за съдържанието, оригиналността им и за грешки, допуснати по тяхна вина.

ISBN 978-954-23-0593-4

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Аспирант Бортэ Григорий,
аспирант Склифос Константин,
магистр Виталий Спынаки
Молдавская Экономическая Академия – Кишинев

Несмотря на то, что о киберпреступности и угрозах безопасности частных данных в последнее время говорят всё чаще и чаще, количество случаев мошенничества, обмана и преступлений в интернете, ровно как и причинённый ущерб продолжают расти[13]. Примечательно, что никаких новых по своей сути атак, преступлений, правонарушений не появилось, преступники лишь приспособились к новой среде.

Целью данной работы является анализ групп проблем и угроз информационной безопасности пользователей в сети интернет с точки зрения электронной коммерции.

Среди наиболее распространённых на данный момент угроз можно выделить следующие:

Мошенничество – одна из самых старых, и в то же время самых распространённых и эффективных[2][5] угроз. Людям обычно предлагается купить какой-либо товар, услугу или каким-нибудь другим образом отдать свои деньги, и не получить взамен совсем не то, что ожидается или ничего вообще. Из наиболее распространённых видов мошенничества в данной категории можно выделить следующие:

• Финансовые пирамиды[8][7]. Это мошенничество было распространено ещё до появления интернета и ничего нового не привнесло. Суть заключается в привлечении новых жертв для выплаты денег предыдущим жертвам.

• „Волшебные кошельки”, данный вид мошенничества характерен по большей части для русскоязычной части интернета.

• „Нигерийские письма”[1], также известные, как 419. Жертве предлагается отправить или собственноручно привезти деньги а в обмен обещается награда куда большего размера.

• Фишинг представляет собой попытку получения пользовательских данных путём выдачи себя за добросовестную сущность[16].

DoS атаки – суть угрозы заключается в предотвращении доступа к определённым ресурсам или услугам[3][4]. На данный момент отказ в обслуживании - пожалуй, самый распространённый и развитый вид атаки. Особенно наглядно это было продемонстрировано во время так

называемой „операции: расплата”[11], во время которой группа обычных пользователей смогла вызвать отказ в обслуживании таких гигантов, как Mastercard, Visa, PayPal. Примечательно, что подобного рода атаки тоже совершенно не новы, по своей природе они сходны с забастовками[2]. Данный метод довольно прост в применении и ужасающе эффективен.

Кража интеллектуальной собственности – или так называемое пиратство. Незаконное распространение и продажа материалов, защищенных законом об авторском праве. В отличие от реального мира, природа информационного пространства устроена таким образом, что копии данных создавать очень легко, и очень тяжело бороться с их распространением[2]. Однако, данный вид преступлений наносит значительные убытки правообладателям. Согласно исследованию Фрэнка Аренса, индустрия теряет около 250 миллиардов долларов в год по вине пиратства[9]. Однако некоторые исследователи критически высказываются об этой цифре[15].

Кража личности – суть преступления заключается в попытке выдать себя за другого человека. Исследователи отмечают спад на 28% в данной области преступлений в 2010 году[12] со ссылкой на статистические данные datalossdb[6], даже несмотря на то, что общее число жалоб в интернете проявляет тенденцию к росту, отмеченную центром по приёму жалоб в интернете[10].

Кража бренда – попытка выдать себя за какой-либо уже известный и раскрученный бренд[2]. Очень часто, данное преступление является целью фишинговых атак[16].

Физическое разрушение – даже самый программно защищённый сервер всё равно может оставаться уязвимым к физическому воздействию[2].

Вандализм – умышленное внесение существенных изменений или же полная замена каких-либо страниц сайта. Обычно, в качестве цели преследуется хвастовство. Реже, в качестве цели выступает реклама, или желание указать на недостатки в работе веб-страницы[2].

Анализ траффика – под анализом трафика подразумевается анализ не содержимого отсылаемых сообщений, а их характеристик[2]. Например, длина сообщений, периодичность их появления, тенденции и отклонения.

Базы данных – суть данной угрозы заключается в хранении персональных данных [2]. Это могут быть как и государственные, например, полицейские базы данных, так и частные хранилища данных, например, клиентов. Проблема заключается в том, что подобные базы могут стать доступны публике, что может способствовать краже личности. Согласно базе данных Chronology of Data Breaches, с начала 2005 года по февраль

2011 года, в открытом доступе находились более половины миллиарда записей, содержащих персональные данные[14].

Слежение – данная проблема заключается в возможности следить за действиями пользователей в интернете[2]: собирать данные о покупках, посещениях страниц. С одной стороны, это удобно для пользователей, им проще просматривать свою историю действий, искать просмотренные материалы, интернет-магазины могут отображать товары, в которых пользователь может быть заинтересован. С другой стороны, утечка таких данных может оказать крайне негативные последствия как для личной жизни, так и послужить мощным инструментом, предоставляющим обширные возможности для кражи личности.

Из наиболее распространённых методов борьбы с перечисленными угрозами для пользователей хотелось бы выделить следующие:

Информирование. Чаще всего, пользователи ведутся на мошенничество благодаря тому, что незнакомы с мошеннической схемой. Проводя специализированные тренинги и семинары можно было бы увеличить степень осведомлённости в области информационных угроз среди групп риска.

Осторожность при отправке своих личных данных. Недобросовестные организации могут разглашать частную информацию, или она может становиться доступной в результате халатного отношения к защитным механизмам.

Для организаций же важно строгое и неукоснительное соблюдение инструкций, предписаний, нормативов и стандартов. Помимо этого, очень важно грамотное проектирование систем защиты, регулярное проведение тренингов, семинаров.

Вновь хотелось бы подчеркнуть, что новых угроз, как таковых, не появилось. Злоумышленники лишь начали использовать новые инструменты, адаптируясь к новой среде. Важно уметь разглядеть за новым „лицом” старую сущность угрозы и предпринять нужные меры.

Библиография

1. Barbara Mikkelson, *Nigerian Scam*, http://www.snopes.com/fraud/advancefee/nigeria.asp
2. Bruce Schneier, *Secrets and Lies*, ISBN 0-471-25311-1
3. CERT, *Denial of Service Attacks*, http://www.cert.org/tech_tips/denial_of_service.html
4. Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, *Distributed Denial of Service Attacks*, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

5. Consumerfraudreporting.org, *Internet Fraud, Scam and Crime Statistics – 2009,* http://www.consumerfraudreporting.org/internet_scam_statistics.htm

6. datalossdb, *Statistics*, http://datalossdb.org/statistics

7. Debra A. Valentine, *Pyramid Schemes*, http://www.ftc.gov/speeches/other/dvimf16.shtm

8. Federal Bureao of Investigation, *Common Fraud Schemes*, http://www.fbi.gov/scams-safety/fraud/fraud#pyramid

9. Frank Ahrens, *U.S. Joins Industry in Piracy War*, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402071.html

10. Internet Crime Complaint Center, *2009 Internet Crime Report*, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

11. Jaikumar Vijayan, *MasterCard, Visa others hit by DDoS attacks over WikiLeaks*, http://www.computerworld.com/s/article/9200521/Update_MasterCard_Visa_others_hit_by_DDoS_attacks_over_WikiLeaks

12. Michelle Singletary, *Identity-theft statistics look better, but you still don't want to be one*, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/09/AR2011020906829.html

13. Ponemon, *First Annual Cost of Cyber Crime Study*, July 2010

14. Privacy Rights Clearinghouse, *Chronology of Data Breaches*, http://www.privacyrights.org/sites/default/files/static/Chronology-of-Data-Breaches_-_Privacy-Rights-Clearinghouse.pdf

15. Richard Menta, *Movie and Record Industry Piracy Figures Incendiary, But Not Fact*, http://www.mp3newswire.net/stories/6002/250billion.html

16. Technical Info, *The Phishing Guide*, http://www.technicalinfo.net/papers/Phishing.html