TECHNOLOGIA ŻYWNOŚCI

INNE

AGROEKONOMIA, AGROTURYSTYKA I ZARZĄDZANIE

Karol KRÓL
Dawid BEDLA

EPISTEME
22/2014, t. I
s. 5-13
ISSN 1895-2241

ANALIZA WYBRANYCH ZAGROŻEŃ ZWIĄZANYCH Z PROMOWANIEM, SPRZEDAŻĄ I REZERWACJĄ USŁUG AGROTURYSTYCZNYCH W INTERNECIE – STUDIUM PRZYPADKU

RISKS ANALYSIS OF THE PROMOTION, SALE AND RESERVATION OF THE AGROTOURISM SERVICES IN THE INTERNET – A CASE STUDY

Abstrakt: Internet stanowi dynamicznie rozwijający się kanał dystrybucji różnego rodzaju towarów i usług. Oprócz ich bezpośredniej sprzedaży służy informowaniu i promocji. Zalety te zostały docenione przez gospodarstwa agroturystyczne, których właściciele co raz częściej wymieniają Internet jako najważniejsze źródło pozyskiwania klientów. Korzystanie z sieci Internet wiąże się jednak z coraz poważniejszymi zagrożeniami, na które są narażeni nie tylko właściciele stron internetowych ale również ich użytkownicy, w tym klienci poszukujący „wczasów pod gruszą". Celem artykułu jest ocena zagrożeń na które narażeni są właściciele gospodarstw agroturystycznych wykorzystujący Internet do promocji, sprzedaży i rezerwacji swoich usług. Przykładem takich zagrożeń są: próby wyłudzenia informacji, ataki szkodliwego oprogramowania czy oszustwa o charakterze przestępstw gospodarczych, które w realny sposób mogą przyczynić się do powstania strat finansowych.
Słowa kluczowe: *zagrożenia w Internecie, szkodliwe oprogramowanie, wyłudzanie informacji*

Abstract: The Internet is now a rapidly growing sales channel for different types of goods and services. In addition to direct sales or reservations, Internet is common used to inform and promotion. These advantages are also recognized by the farmhouses, whose owners more often used the Internet as a major source of customer acquisition. Using the Internet is associated with increasing dangers on which exposed are not only the owners of websi-

tes but all users. The purpose of this article is to evaluate the risks, which in real way they can contribute to financial losses, attempts extorting, malware attacks and fraudulent nature of direct economic crimes, on which are exposed website owners tourist farms.
Key words: *threats on the Internet, malware, phishing*

WSTĘP

Szacuje się, że statystycznie więcej niż co trzeci mieszkaniec globu korzysta z Internetu. W przeliczeniu na populację to niemal 2,4 mld osób. Systematycznie rośnie liczba użytkowników Internetu w Unii Europejskiej. W 2012 r. dostęp do sieci zadeklarowało 75% jej mieszkańców [Report 2013]. W Polsce dostęp do Internetu w miejscu zamieszkania deklaruje 70,5% gospodarstw domowych [IAB 2012].

Internet stosunkowo szybko stał się czwartym, masowym źródłem społecznego przekazu. Coraz tańszy i ogólnodostępny, stanowi wyposażenie większości gospodarstw domowych zarówno w mieście, jak i na wsi. Barrow [2006, s. 11] nie pozostawia złudzeń, cyt. „Internet stał się faktem". Zastosowanie Internetu jako narzędzia promocji i sprzedaży usług nie ominęło sektora turystyki wiejskiej. Własną stronę internetową posiada już większość gospodarstw agroturystycznych. Liczne wykorzystują portale społecznościowe, blogi, katalogi i komunikatory oraz honorują płatności i rezerwacje internetowe. Wszystkie te operacje usprawniają prowadzenie działalności gospodarczej oraz wyszukanie i zakup usługi przez klientów, jednocześnie wystawiając użytkowników na zagrożenia. Największe firmy zajmujące się bezpieczeństwem w Internecie prognozują wzrost liczby niebezpieczeństw w sieci. Dwornik [2013] przekonuje, że wraz z upowszechnianiem dostępu do Internetu coraz częstsze będą próby kradzieży i wyłudzeń poufnych informacji, a metody stosowane przez oszustów będą co raz bardziej wyszukane.

MATERIAŁ I METODY

Celem pracy jest analiza opisowa oraz subiektywna ocena punktowa wybranych zagrożeń występujących w Internecie, na które narażeni są właściciele gospodarstw agroturystycznych wykorzystujący Sieć do promocji, rezerwacji oraz sprzedaży swoich usług. Szczególną

uwagę poświęcono zagrożeniom mogącym przyczynić się do powstania strat finansowych. W pracy przedstawiono mechanizm działania oszustów. Ponadto wykonano studia przypadków (ang. *case study*) tj. konkretnych zagrożeń występujących w Internecie oraz opisano sposoby ich uniknięcia. Studium przypadku to metoda rozpowszechniona w latach 90. XX wieku [Longley 1999] a jej głównym celem jest przedstawienie i analiza konkretnego zjawiska [Piekkari i Welch 2011].

Zagrożenia występujące w Internecie można podzielić na mniej lub bardziej poważne w skutkach. Niektóre mogą doprowadzić do utraty środków finansowych. Inne bywają jedynie uciążliwe, np. „spam". Z punktu widzenia techniczno-organizacyjnego zagrożenia dzielimy na te, za które odpowiadają aplikacje (roboty sieciowe, programy komputerowe) i te, za którymi stoi bezpośrednio człowiek. W przypadku tych ostatnich są to: próby wyłudzania poufnych informacji osobistych w tym kradzież tożsamości (ang. *phishing, pharming, spearphishing*), ataki złośliwego oprogramowania (ang. *malware, spyware*), ataki na strony internetowe typu wstrzyknięcie złośliwego kodu (ang. *HTML injection*), próby oszustw internetowych bazujące na ukrywaniu istotnych klauzur w obszernych regulaminach usług lub oparte o informacje pozyskane w Internecie, wreszcie przemoc bezpośrednia (ang. *cyberbullying*) i pornografia (tab. 1).

Tab. 1. Charakterystyka wybranych zagrożeń występujących w Internecie

Phishing	W wolnym tłumaczeniu oznacza „łowienie w sieci" lub „łowienie siecią". Wyłudzanie poufnych informacji osobistych poprzez podszywanie się pod zaufaną osobę lub instytucję np. bank, portal aukcyjny lub społecznościowy. Próby oszustwa opierają się na wiadomości e-mail, w której zawarta jest prośba o bezpośrednie udostępnienie haseł dostępu lub podanie ich na spreparowanej stronie internetowej, do której zwykle prowadzi odsyłacz zawarty w treści wiadomości. Próba oszustwa ma charakter zautomatyzowany, masowy i globalny.
Pharming	Forma phishingu. Próba oszustwa polegająca na wyłudzenia danych autoryzacji dostępu poprzez fałszywą stronę internetową. Wymaga, aby komputer użytkownika był zainfekowany programem typu koń trojański lub zatrucia systemu nazw domenowych. Gdy komputer użytkownika jest zainfekowany, pomimo wpisana prawidłowego adresu strony internetowej zostaje on przeniesiony na fałszywą. Atak ma na celu przejęcie wpisywanych przez użytkownika haseł, numerów kart kredytowych i innych poufnych informacji.

Spear phishing	W wolnym tłumaczeniu oznacza „łowienie harpunem". Forma phishingu. Próba wyłudzenia poufnych informacji za pomocą ukierunkowanej wiadomości e-mail. Oszust wykorzystuje informacje związane z potencjalną ofiarą pozyskane np. z portali społecznościowych. Wiadomość jest przygotowana tak, aby sprawiała wrażenie wysłanej przez osobę, firmę lub instytucję znaną odbiorcy. Zwykle nadawca wiadomości podszywa się pod wybranego użytkownika Internetu posługując się personaliami oraz fotografią pozyskanymi w sieci.
Malware	Złośliwe oprogramowanie o szkodliwym działaniu. Wirusy, robaki, programy szpiegujące, konie trojańskie i inne. Często infekuje strony internetowe, które wykorzystuje do rozpowszechniania złośliwego oprogramowania wśród odwiedzających ją użytkowników. Złośliwe oprogramowanie może być instalowane przez zainfekowane strony internetowe, programy pobierane z sieci albo instalowane z dysku CD, DVD lub innych nośników danych.
Spyware	Programy, których celem jest zbieranie informacji o działaniach podejmowanych przez użytkowników komputera lub urządzeń mobilnych podejmowanych w sieci Internet. Często zbierane są również dane personalne lub inne informacje poufne. Gromadzą informacje o użytkowniku, często bez jego zgody, wiedzy i kontroli przekazują je twórcy programu.
Inne	HTML injection, przemoc w Internecie ang. cyberbullying (ataki słowne, szykany, pomówienia, złośliwe komentarze i inne umieszczane na portalach społecznościowych), utrata danych z komputera, złośliwe aplikacje w serwisach społecznościowych, cyber-terroryzm (ataki botnet).

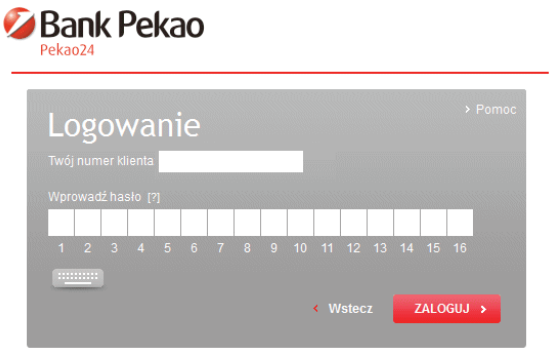
Źródło: opracowanie własne na podstawie raportu „Bezpieczeństwow Internecie" [Dwornik 2013]

WYNIKI I WNIOSKI

Studium przypadku – phishing, pharming, spear phishing

Władysław i Janina Nowak prowadzą gospodarstwo agroturystyczne w okolicach Olsztynka (woj. warmińsko-mazurskie). Działalności turystycznej sprzyja lokalizacja gospodarstwa w okolicy jezior Mielno i Omen. Wypoczynek polecają pasjonatom wędkarstwa, sportów wodnych, rowerzystów i miłośników jazdy konnej. Nastoletni syn państwa Nowak prowadzi stronę internetową oraz profil gospodarstwa na portalu społecznościowym. Przed sezonem letnim,

państwo Nowak podjęli decyzję o zakupie aparatu fotograficznego. Syn namówił ich do zakupu i płatności przez Internet, po czym informację zamieścił na portalu społecznościowym. Następnego dnia otrzymał wiadomość e-mail o treści: „Szanowni Państwo Władysław i Janina Nowak! Gratulujemy zakupu aparatu fotograficznego. Z przykrością informujemy, że nie odnotowaliśmy wpłaty. Aby otrzymać zakupiony towar prosimy o zalogowanie się do konta i potwierdzenie wykonania przelewu (ryc. 1). Odnośnik zamieszczamy poniżej. Zakupiony towar zostanie wysłany natychmiast po zweryfikowaniu płatności. Dziękujemy za zakup aparatu w naszym sklepie". Syn państwa Nowak w przysłanym formularzu wpisał numer klienta oraz wprowadził hasło. Tego samego dnia z konta bankowego rodziców wypłacono wszystkie pieniądze.



Ryc. 1. Przykład spreparowanego formularza logowania się do bankowości internetowej (wszystkie pola hasła są wymagane)
Źródło: opracowanie własne na podstawie formularza Banku Pekao SA

W opisywanym przypadku mamy do czynienia z próbą oszustwa typu ang. *spear phishing*, z wykorzystaniem spreparowanej strony internetowej ang. *pharming*. Oszuści dysponowali wiedzą o personaliach ofiary oraz czynnościach związanych z zakupem aparatu fotograficznego i podszyli się pod pracownika sklepu internetowego. Informacje czerpali z obserwacji konta na portalu społecznościowym ofiary, do którego dostęp uzyskali dzięki utworzeniu fikcyjnego profilu, podszywając się po jednego z przyjaciół rodziny. Użytkownik w formularzu logowania został poproszony o podanie numeru klienta oraz hasła w całości (ryc. 1). Próba wyłudzenia może być również

ukryta pod pretekstem prośby o zresetowanie hasła lub ponowną weryfikację numerów karty kredytowej.

STUDIUM PRZYPADKU – MALWARE, SPYWARE

Wiesław i Dorota Kowalczyk prowadzą gospodarstwo agroturystyczne w okolicy Radziszowa (woj. małopolskie). Gospodarstwo wyróżnia się ofertą skierowaną do osób starszych gwarantując indywidualną dietę, okresowe wizyty lekarskie oraz sprzęt do rehabilitacji ruchowej i hydromasażu. Gospodarze udostępniają swój adres e-mail na stronie internetowej gospodarstwa. Spośród licznych wiadomości Wiesław Kowalczyk dostrzegł zapytanie ofertowe od klienta. Klient przekonywał, że jest zainteresowany dłuższym pobytem w gospodarstwie, a swoje zapytanie zawarł w pliku PDF dołączonym do wiadomości. Pomimo licznych prób otwarcia załącznika operacja się nie powiodła a system operacyjny zaczął pracować niestabilnie. Po ponownym uruchomieniu komputera na ekranie monitora pojawił się komunikat, że pliki umieszczone na dysku zostały zaszyfrowane i zablokowane. W komunikacie zawarto informację o możliwości ich odzyskania po uiszczeniu opłaty w wysokości 300 €.

Komputer państwa Kowalczyk został zainfekowany *koniem trojańskim* z rodzaju *Filecoder* (ang.). Atak nastąpił poprzez spreparowaną wiadomość e-mail. Złośliwa aplikacja została uruchomiona przy próbie otwarcia zainfekowanego dokumentu PDF. *Filecoder szyfruje* pliki znajdujące się na dysku komputera. Ich odblokowanie wiąże się z opłaceniem okupu w wyznaczonym czasie. Nie wniesienie opłaty skutkuje usunięciem plików. W opisywanym przypadku mamy do czynienia z atakiem typu ang. *malware*, z wykorzystaniem ukierunkowanej wiadomości e-mail. W przypadku nowych odmian *koni trojańskich* posiadanie antywirusa może być niewystarczające. Atak może nastąpić m.in. poprzez: zainfekowaną stronę internetową, instalację oprogramowania użytkowego niepewnego pochodzenia lub przy pobieraniu nielegalnych plików z niesprawdzonych źródeł.

Tab. 2. Ocena wybranych zagrożeń w Internecie. Skala punktowa 1-10.

	Skala niebezpieczeństwa	Trudność prze-prowadzenia ataku	Prawdopodobieństwo		Ogólna ocena
			zaistnienia ataku	powodzenia ataku	
Phishing	4	4	8	4	4
	Komentarz: niebezpieczeństwo strat finansowych spowodowane atakiem jest relatywnie nieduże z uwagi na ogólny i zwykle niedopracowany charakter wiadomości kierowanych do użytkowników Internetu. Atak jest relatywnie łatwy do przygotowania gdyż większość wiadomości jest tworzona i rozsyłana przez roboty sieciowe i nie ma charakteru ukierunkowanego na konkretną osobę lub grupę osób.				
Spear phishing	8	8	4	7	7
	Komentarz: niebezpieczeństwo strat finansowych spowodowane atakiem jest relatywnie duże z uwagi na próby wyłudzeń loginów i haseł do prywatnych kont lub numerów kart kredytowych. Atak jest ukierunkowany i relatywnie trudny do przeprowadzenia gdyż wymaga bezpośredniego zaangażowania oszustów. Z uwagi na trudność przygotowania ataku prawdopodobieństwo jego zaistnienia jest nieduże, aczkolwiek rośnie proporcjonalnie do majątku potencjalnej ofiary.				
Malware	6	4	8	6	6
	Komentarz: niebezpieczeństwo strat finansowych spowodowane atakiem jest relatywnie duże z uwagi na próby wyłudzeń loginów i haseł do prywatnych kont lub numerów kart kredytowych. Prawdopodobieństwo ataku i jego powodzenia jest duże ponieważ złośliwe oprogramowanie występuje powszechnie, może być przenoszone na dowolnym nośniku danych cyfrowych oraz rozpowszechniane w Internecie.				
Spywre	6	4	8	8	6
	Komentarz: niebezpieczeństwo strat finansowych spowodowane atakiem jest relatywnie duże z uwagi na próby wyłudzeń loginów i haseł do prywatnych kont lub numerów kart kredytowych. Prawdopodobieństwo ataku i jego powodzenia jest duże. Większość komputerów jest zainfekowana mniej lub bardziej poważnymi aplikacjami typu spyware.				

Źródło: ocena własna

PODSUMOWANIE

W artykule przedstawiono wybrane zagrożenia występujące w Internecie na przykładzie gospodarstw agroturystycznych. Ataki przeprowadzane za pośrednictwem Sieci często okazują się być przemyślane i kompleksowe, a oszuści wykorzystują wiedzę o zachowaniach społecznych człowieka, czerpiąc z dokonań psychologów i socjologów. Złośliwe oprogramowanie stanowi zagrożenie dla wszystkich użytkowników komputerów i urządzeń mobilnych. Bywa jednak, że jest tworzone z myślą o infekowaniu konkretnego systemu operacyjnego lub jego komponentów. Próby wyłudzeń poufnych informacji generowane przez aplikacje sieciowe mają często charakter globalny i masowy. Ataki bezpośrednie są zwykle bardziej wyszukane i wymierzone w konkretnych odbiorców.

W praktyce instytucje, które wymagają uwierzytelniania w procesie logowania (potwierdzenie tożsamości) nigdy nie proszą o podanie pełnego hasła do serwisu internetowego. Przestrzegają przed używaniem do logowania odnośników przesyłanych w wiadomościach e-mail lub SMS. Zalecają ostrożność w stosunku do wiadomości pochodzących od nieznanych nadawców, które zawierają załączniki.

Większości zagrożeń występujących w Internecie można uniknąć kierując się zasadą ograniczonego zaufania oraz zdrowego rozsądku. Podstawową metodą obrony przed atakami jest profilaktyka oraz świadome użytkowanie narzędzi i technik komputerowych. Zagrożeń występujących w Internecie można uniknąć również poprzez ograniczone udostępnianie informacji osobistych. Liczne portale społecznościowe zachęcają do rejestracji, przy której wymagają od użytkownika podania danych osobowych, zainteresowań, preferencji konsumenckich, powiązań rodzinnych oraz zawodowych i wiele innych. Użytkownicy często bez rozwagi udostępniają nieznajomym prywatne dane a zjawisko to staje się coraz bardziej powszechne. W obronie przed zagrożeniami występującymi w Internecie pomocne są programy antywirusowe oraz zapory sieciowe tj. programy typu ang. *firewall*, jednak żadne oprogramowanie komputerowe nie zastąpi zasady ograniczonego zaufania.

LITERATURA

Barrow C. 2006. *Biznes w sieci*. Wydawnictwo Felberg SJA. Warszawa, s. 11.
Dwornik B. 2013. *Hakerzy zmienili front*. Bezpieczniej nie będzie [w] Raport Bezpieczeństwo w Internecie. Wydawca: Interaktywnie.com Sp. z o.o. Wrocław, s. 7-9.
IAB. 2012. *Raport Strategiczny IAB Polska*. Internet 2012 – Polska, Europa, świat. Media & Marketing Polska. Dodatek specjalny. 10. Wydanie Jubileuszowe. Wydawca VFP Communications Sp. z o.o. Warszawa. s. 18.
Langley A. 1999. *Strategies for theorizing from process data*. Academy of Management Review. t. 24, nr 4: 691-710.
Piekkari R. Welch C. 2011. *Rethinking the Case Study in International Business and Management Research*, Edward Elgar, Cheltenham, s. 5.
Report. 2013. *Cyber security. Special Eurobarometer 404.* Conducted by TNS Opinion & Social at the request of the European Commission, Directorate-General Home Affairs, s. 4.

Adres do korespondencji:

dr inż. Karol Król
Katedra Gospodarki Przestrzennej i Architektury Krajobrazu
Wydział Inżynierii Środowiska i Geodezji
Uniwersytet Rolniczy w Krakowie
Al. Mickiewicza 24/28, p. 208, 30059 Kraków
e-mail: k.krol@ur.krakow.pl

dr inż. Dawid Bedla
Katedra Ekologii, Klimatologii i Ochrony Powietrza
Wydział Inżynierii Środowiska i Geodezji
Uniwersytet Rolniczy w Krakowie
e-mail: d.bedla@ur.krakow.pl