Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Wydział Informatyki i Zarządzania
Politechnika Wrocławska

Świadczenie usług drogą elektroniczną w aspekcie zagrożeń

1. Wstęp

W dobie dynamicznego rozwoju gospodarki elektronicznej działalność niemal każdej organizacji, w tym administracji publicznej i służby zdrowia, jest prowadzona przy wykorzystywaniu systemów teleinformatycznych, zatem konieczna jest dbałość o ich niezawodność i bezpieczeństwo. Świadczenie usług drogą elektroniczną wymaga znajomości oraz przestrzegania obowiązujących przepisów prawnych, stosowania przyjętych procedur zbierania, przetwarzania i archiwizowania danych.

Poziom ochrony systemu teleinformatycznego, w tym danych i aplikacji realizujących usługi sieciowe, zależy od wielu czynników: od samego projektu i jego implementacji, wdrożonego systemu zabezpieczeń, administrowania i eksploatacji. Zagrożenia dla bezpiecznego użytkowania mogą być przypadkowe (awaria sprzętu i błędy ludzkie) lub celowe (działania osób nieuprawnionych wyrządzające szkody). Możliwość podejmowania skutecznych ataków na system wynika przede wszystkim z błędów oprogramowania, błędów konfiguracji oraz dostępności narzędzi do bezprawnych działań. Popularne metody atakowania systemów to: manipulowanie parametrami transmisji, SQL Injection, ataki CSRF (*Cross Site Request Forgeries*) i XSS (*Cross-Site Scripting*), umożliwiające przekazanie szkodliwego kodu lub przekierowanie na fałszywą stronę internetową, oraz ataki na proces uwierzytelnienia czy sesję użytkownika.

Zagrożenie dla bezpieczeństwa sieciowego stanowi poważny problem, który w szczególnym stopniu dotyczy systemów informatycznych w ochronie zdrowia i administracji publicznej z uwagi na gromadzenie, przetwarzanie i transmisję

danych osobowych wrażliwych lub poufnych. Wszelkie stosowane na różnych płaszczyznach sposoby zabezpieczeń, takie jak zapory sieciowe, oprogramowanie antywirusowe, dbałość o aktualizację oprogramowania, a nawet zaawansowane metody kryptograficzne dla ochrony danych, nie rozwiązują problemu całkowicie.

Rządowy program informatyzacji państwa przewiduje podnoszenie jakości usług świadczonych drogą elektroniczną i dalszy ich rozwój, szczególnie w sektorze administracji publicznej i ochronie zdrowia. Powszechna realizacja tych usług jest ściśle uzależniona od opracowywania nowych i dostosowywania obowiązujących stosownych przepisów prawnych.

Celem artykułu jest przedstawienie rozwoju wybranych usług świadczonych drogą elektroniczną, a także realnych dla nich zagrożeń, przy jednoczesnym podkreśleniu skali tego zjawiska, wynikającego z problemów zabezpieczania systemów teleinformatycznych na odpowiednio wysokim poziomie.

2. Elektroniczne usługi publiczne

Rozwój usług sieciowych charakteryzuje bardzo duża dynamika powodowana atrakcyjnością i wygodą ich realizacji, do czego przyczynia się także coraz większa popularność urządzeń mobilnych. Zgodnie z ustawą z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204; UŚUDE) i jej nowelizacją z 7 listopada 2008 r. (ustawą o zmianie ustawy o świadczeniu usług drogą elektroniczną, Dz. U. z 2008 r. Nr 216, poz. 1371), usługa elektroniczna (e-usługa) wiąże się z przekazywaniem danych na odległość na żądanie usługobiorcy (bez konieczności jednoczesnej obecności obu stron) z wykorzystaniem urządzeń elektronicznego przetwarzania, odpowiedniego oprogramowania i sieci telekomunikacyjnej. W ustawie tej zdefiniowane są także zasady prowadzenia e-usług i reagowania na zachowania niezgodne z prawem. Nowelizacja ustawy z 12 lipca 2013 r. (ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, Dz. U. z 2013 r. Nr 0, poz. 1036) zawiera zmiany dotyczące zapewnienia wolności w Internecie, a jednocześnie szeroko rozumianego bezpieczeństwa danych, m.in. obejmuje procedurę zgłaszania i usuwania bezprawnych treści (*notice and take down*). Spośród wielu organów uprawnionych do kontroli legalności usług elektronicznych szczególne znaczenie mają: Generalny Inspektor Ochrony Danych Osobowych (GIODO), Rzecznik Praw Obywatelskich (RPO), Prokuratura oraz Najwyższa Izba Kontroli (NIK).

Realizację e-usług umożliwiają np. serwisy informacyjne, bankowość elektroniczna, e-aukcje, sklepy i księgarnie internetowe, biblioteki cyfrowe, systemy rezerwacji (np. terminów wizyt w ZUS, urzędzie miasta czy wizyt lekarskich). Do najpopularniejszych obecnie usług elektronicznych należą usługi bankowe i finansowe, informacyjne, kupna/sprzedaży, rezerwacji miejsc (np. hotelowych, lotniczych, na imprezy kulturalne i turystyczne).

Duży nacisk kładzie się na rozwój e-usług w administracji publicznej[1] i w ochronie zdrowia. Akty prawne opublikowane w wydawnictwach urzędowych (Dzienniku Ustaw i Monitorze Polskim wydawanych przez prezesa Rady Ministrów), dostępne są przez Internetowy System Aktów Prawnych[2]. W społeczeństwie informacyjnym załatwianie spraw urzędowych przy wykorzystaniu Internetu (niezależnie od miejsca przebywania) wydaje się usługą podstawową i powinno być powszechnie stosowane.

Zgodnie z ustawą z 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2010 r. Nr 40, poz. 230), od 17 czerwca 2010 r. wszystkie podmioty świadczące usługi publiczne są zobowiązane do umożliwienia interesantom składania wniosków w postaci elektronicznej przez Elektroniczną Skrzynkę Podawczą (ESP), udostępnioną w ramach usług ePUAP (Elektronicznej Platformy Usług Administracji Publicznej, epuap.gov.pl). Zainteresowane podmioty publiczne mogą przyjmować wnioski od obywateli przez ESP bez konieczności tworzenia w tym celu własnych stron WWW. Usługi z wykorzystaniem Elektronicznej Skrzynki Podawczej oferuje m.in. Narodowy Fundusz Zdrowia (NFZ). Za pośrednictwem ePUAP można też zweryfikować dane dotyczące dowodów rejestracyjnych i praw jazdy zawartych w bazie CEPiK (Centralnej Ewidencji Pojazdów i Kierowców). Planowane zmiany ustawy przewidują wprowadzenie obowiązku posługiwania się Elektroniczną Skrzynką Podawczą przez wszystkie podmioty publiczne.

Korzystanie z usług ePUAP jest bezpłatne, wymaga jednak założenia konta i profilu zaufanego, wykorzystywanego w procesie potwierdzania tożsamości użytkownika. Profil zaufany można założyć osobiście w wybranym miejscu (np. w ZUS, urzędzie skarbowym, biurze meldunkowym) lub przesłać wypełniony wniosek wraz z potwierdzeniem tożsamości (podpisem elektronicznym)

[1] D. Adamski, P. Litwiński, C. Martysz, Z. Okoń, G. Sibiga, R. Szostak, D. Szostek, M. Świerczyński, *E-administracja. Prawne zagadnienia informatyzacji administracji*, PRESSCOM, Wrocław 2009.

[2] Internetowy System Aktów Prawnych, isap.sejm.gov.pl (data dostępu 5.11.2013).

przez Internet. Lista usług udostępnianych przez ePUAP nie obejmuje jeszcze wszystkich potrzeb obywateli (np. nie ma możliwości złożenia wniosku o wydanie paszportu czy dowodu osobistego). Ponadto, czas realizacji niektórych usług nadal jest zbyt długi (np. uzyskania odpisu aktu stanu cywilnego).

14 czerwca 2012 r. na ePUAP została uruchomiona Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (pue.zus.pl) – pierwszy w Polsce w pełni zrealizowany projekt e-administracji. Portal umożliwia obywatelom dostęp do ich danych zgromadzonych na kontach ZUS, a także generowanie oraz przesyłanie pism i dokumentów drogą elektroniczną.

Wdrożony w styczniu 2013 r. system eWUŚ (Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców) umożliwia sprawdzenie uprawnień pacjenta do korzystania z opieki zdrowotnej finansowanej ze środków publicznych. Niestety, zarówno temu systemowi, jak i innym wdrożonym w ochronie zdrowia nie zapewniono ciągłości działania (zbyt często mają miejsce przerwy techniczne i konserwatorskie). Z dniem 1 sierpnia 2014 r. w Polsce zostanie nałożony obowiązek prowadzenia dokumentacji medycznej w postaci elektronicznej, a dane o usługach medycznych pacjentów będą umieszczane w systemie eWUŚ automatycznie. Generalny inspektor ochrony danych osobowych zwrócił uwagę na szczególną ochronę tych danych, których pozyskanie jest cenne dla różnych podmiotów, np. dla firm ubezpieczeniowych. Dostęp do nich przez Portal Świadczeniodawcy będą mieli m.in. lekarze z podpisanymi stosownymi umowami. Warto podkreślić, że w innych krajach (np. w Holandii) dane medyczne są przechowywane w systemach informatycznych dostępnych przez Internet jedynie po wyrażeniu na to zgody przez pacjenta.

Dużym problemem było istnienie kilkudziesięciu rodzajów rejestrów medycznych bez prawnie określonych uprawnień dostępu do nich, niewspółdziałających ze sobą i bez możliwości świadczenia e-usług. Od lipca 2012 r. ich liczbę ograniczono, pozostawiając tylko zbiory niezbędne. W styczniu 2013 r. w ramach projektu P2 („Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych”[3]) na stronie Centrum Systemów Informacyjnych Ochrony Zdrowia udostępniono usługi kilku rejestrów medycznych, zapewniając jednocześnie optymalny poziom bezpieczeństwa danych. Projekt P2 jest ściśle związany z projektem P1 – Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych[4].

[3] http://wartowiedziec.org/index.php/zdrowie/zarzadzanie/10232-wszystko-o-projekcie-p2 (data odczytu 25.10.2013).

[4] Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych, p1.csioz.gov.pl (data odczytu 5.11.2013).

W systemie P1 (bazowym projekcie w Programie informatyzacji służby zdrowia) będą gromadzone dane o zdarzeniach medycznych przeprowadzanych na terenie Polski, dotyczących obywateli UE. W ramach projektu P1 w 2011 r. w Krakowie wdrożono prototyp Internetowego Konta Pacjenta (ipk.gov.pl), a w Lesznie prototyp e-Recepty. Oba prototypy są nadal w fazie testowania przez serwis zintegrowanych prototypów IKP oraz e-Recepty (system.ikp.gov.pl). W lipcu 2013 r. udostępniono pacjentom portal Zintegrowany Informator Pacjenta[5] (ZIP), realizujący usługi informacyjne dotyczące m.in. sfinansowanych przez NFZ od 2008 r. świadczeń medycznych, wystawionych recept i wniosków sanatoryjnych oraz aktualnego statusu ubezpieczenia zapisanego w systemie eWUŚ.

W sierpniu 2013 r. Komisja Europejska podjęła decyzję o przeznaczeniu 13,7 mln EUR na uruchomiony 1 kwietnia 2013 r. trzyletni projekt e-SENS[6] (*Electronic Simple European Networked Services*). W ramach projektu planowany jest rozwój transgranicznych cyfrowych usług publicznych. Celem przedsięwzięcia jest ułatwienie zakładania i prowadzenia działalności gospodarczej na terenie Unii Europejskiej oraz uproszczenie formalności związanych z zagranicznymi wyjazdami turystycznymi, pracą zawodową, nauką czy zawieraniem związków małżeńskich. Uczestnicy z 20 krajów europejskich realizują wiele różnych projektów związanych m.in. z bezpieczną wymianą informacji w zakresie tożsamości elektronicznej (*Secure idenTity acrOss boRders linKed 2.0* – STORK 2.0), z rozwojem elektronicznych systemów dokumentacji medycznej (*Smart Open Services for European Patients – Open eHealth Initiative for a European* – epSOS), ułatwieniem dostępu do usług prawnych w Europie (e-CODEX) i prowadzeniem działalności on-line (*Pan-European Public Procurement Online* – PEPPOL).

Duże znaczenie ze względu na zniesienie kontroli na granicach państw należących do strefy Schengen ma System Informacyjny Schengen drugiej generacji (rozporządzenie 2006/1987/WE Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji – SIS II). System ten uruchomiono 9 kwietnia 2013 r. i są w nim przechowywane dane (w tym biometryczne) o osobach i przedmiotach (poszukiwanych, zaginionych itp.). Z danych zgromadzonych w tej bazie mogą korzystać organa ścigania, wymiaru sprawiedliwości i administracyjne. Wszystkie kraje Unii Europejskiej

[5] Zintegrowany Informator Pacjenta, zip.nfz.gov.pl (data odczytu 5.11.2013).

[6] *Komisja zapowiada wsparcie w wysokości 13,7 mln euro na transgraniczne cyfrowe usługi publiczne*, komunikat prasowy Komisji Europejskiej, http://europa.eu/rapid/press-release_IP-13-778_pl.htm (data odczytu 5.11.2013).

(z wyjątkiem Danii) mogą korzystać z europejskiej komputerowej bazy danych EURODAC (*European Dactyloscopy*), która zawiera odciski palców imigrantów i osób ubiegających się o azyl w państwach unijnych.

Korzystanie z e-usług często wymaga od użytkownika udostępnienia danych osobowych, co nie zawsze jest uzasadnione. Obecnie w Ministerstwie Spraw Wewnętrznych trwają prace nad opracowaniem ustawy o monitoringu wizyjnym i zagwarantowaniu prawnej ochrony prywatności obywateli przez wzmocnienie mechanizmów kontroli dostępu uprawnionych służb do pozyskiwania i wykorzystywania danych telekomunikacyjnych. W październiku 2013 r. NIK opublikowała raport z kontroli za okres od stycznia 2011 r. do czerwca 2012 r. w zakresie uzyskiwania i przetwarzania danych przez uprawnione podmioty, w którym krytykuje niewłaściwe ich pozyskiwanie z bilingów[7]. Naczelna Izba Kontroli postuluje także wprowadzenie instrumentów gwarantujących trwałe niszczenie danych już niepotrzebnych. W Parlamencie Europejskim są prowadzone prace nad nowymi przepisami dotyczącymi ochrony danych osobowych, m.in. nad sformułowaniem prawa do bycia zapomnianym. Zapewniałyby one użytkownikom większą kontrolę nad danymi pozostawianymi w Internecie oraz obligowałyby administratorów portali internetowych do trwałego ich usuwania (także ich kopii i odniesień do nich). Realizacja techniczna takich przepisów wymagałaby monitorowania wszelkiej działalności w sieci, co nie jest łatwym zadaniem[8].

3. Zagrożenia dla usług sieciowych

Zgromadzone w systemach teleinformatycznych dane oraz usługi realizowane drogą elektroniczną są narażone na różnego typu ataki, których ostatecznym celem mogą być: podszycie się pod autoryzowanego użytkownika, nielegalny dostęp do zasobów systemu lub blokada ich dostępności osobom upoważnionym. Zagadnienie zagrożenia bezpieczeństwa dotyczy wszystkich systemów teleinformatycznych, a skala zjawiska nieustannie rośnie.

---

[7] *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, nr ewid. 107/2013/P/12/191/KPB – wersja jawna (data odczytu 5.11.2013).

[8] B. Pręda, *Wyłączenie odpowiedzialności za udostępnianie linków – uwagi do projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną*, „Kwartalnik Naukowy: Prawo Mediów Elektronicznych" 2012, nr 2, s. 23–25.

Organizacja OWASP (Open Web Application Security Project), której celem jest edukacja w zakresie zagrożeń sieciowych, w publikacji Top 10 2013 zdefiniowała dziesięć najczęściej spotykanych zagrożeń dla bezpieczeństwa aplikacji internetowych. Sklasyfikowano je według częstości występowania, możliwości wykorzystywania, wykrywalności i rozmiaru szacowanych potencjalnych strat[9]. Na czele listy znalazły się ataki SQL Injection (wstrzyknięcie kodu) oraz XSS (pobranie szkodliwego kodu z zainfekowanej strony). W opracowanej metodyce testowania aplikacji webowych opublikowanej jako OWASP Testing Guide[10] opisano testy procesu uwierzytelniania, autoryzacji, walidacji danych, zarządzania sesjami czy mechanizmów AJAX (*Asynchronous JavaScript and XML*)[11] oraz pokazano sposób określania ryzyka dla wykrytych podatności.

Błędy w oprogramowaniu – główna przyczyna zagrożeń bezpieczeństwa sieciowego – są wykorzystywane do atakowania systemów teleinformatycznych przez exploity (programy komputerowe, skrypty) w celu wymuszenia wykonania określonych operacji. Techniki stosowane w exploitach (takie jak przepełnienie bufora lub stosu, błąd formatowania łańcucha znaków) wykorzystują specyficzną cechę architektury komputerów: przechowywanie danych i rozkazów sterujących w tej samej pamięci. Luka w oprogramowaniu, wykryta przez przestępców komputerowych zanim producent opracuje odpowiednią poprawkę, może być wykorzystana do przeprowadzenia ataku Zero-day. Znane exploity przechowywane w bazie Metasploit są przeznaczone do testowania zabezpieczeń, jednak mogą być również wykorzystywane przez przestępców sieciowych.

W marcu 2013 r. firma Secunia opublikowała raport za 2012 r. *Secunia Vulnerability Review 2013* dotyczący liczby wykrytych w tym okresie luk, z którego wynika, że w monitorowanym przez nią oprogramowaniu (2503 aplikacje, 421 wydawców) było ich aż 9776[12]. W ciągu ostatnich kilku lat całkowita liczba rejestrowanych nowych luk utrzymuje się na stałym poziomie, jednak w przypadku popularnych przeglądarek (Chrome, Firefox, Opera, Safari) widoczny jest ich wzrost (rysunek 1), co ma istotne znaczenie, są to bowiem narzędzia umożliwiające użytkownikom kontakt z siecią (a więc także podczas realizacji e-usług). Eksperci przewidują dalszy wzrost ataków na najpopularniejsze programy, szczególnie na aplikacje webowe.

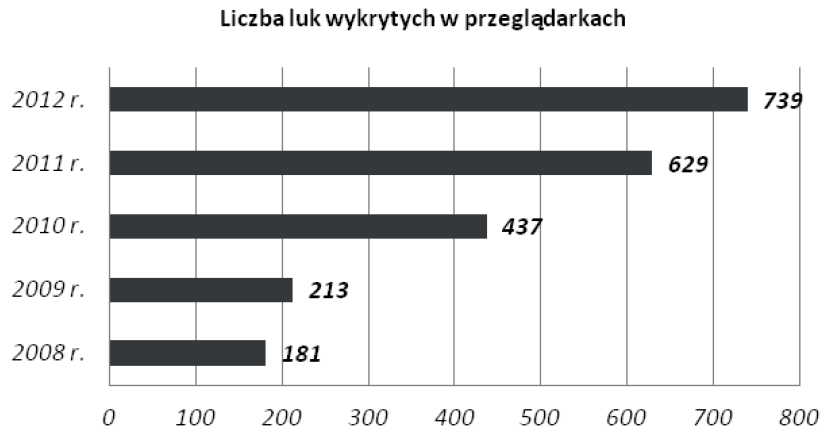
---

[9] www.owasp.org/index.php/Top_10_2013 (data odczytu 5.11.2013).

[10] www.owasp.org/index.php/OWASP_Testing_Project (data odczytu 5.11.2013).

[11] Technika tworzenia aplikacji sieciowych zapewniająca dynamiczną interakcję z użytkownikiem.

[12] http://secunia.com/vulnerability-review/vulnerability_update_all.html (data odczytu 5.11.2013).



Rysunek 1. Liczba luk wykrytych w przeglądarkach internetowych w latach 2008–2012
Źródło: opracowanie własne na podstawie: *Secunia Vulnerability Review 2013*.

Aplikacje realizujące usługi sieciowe zazwyczaj korzystają z danych przechowywanych w relacyjnych bazach danych. By uzyskać do nich dostęp, używają zapytań języka SQL. Jeśli wynik operacji zależy od wprowadzanych danych przez użytkownika (zapytanie SQL jest parametryzowane), a nie zastosowano odpowiednich zabezpieczeń, aplikacja może być podatna na atak SQL Injection, powodujący wykonanie niedozwolonej operacji. Skutkiem takiego ataku (niewykrywanego przez oprogramowanie ochronne czy zaporę sieciową) może być:

- uzyskanie informacji o danym systemie bazodanowym,
- nieautoryzowany dostęp do danych (najczęstszy cel ataku),
- modyfikacja danych, ich dodanie lub usunięcie,
- uszkodzenie bazy danych lub wyłączenie serwera bazodanowego,
- zdalne wykonanie polecenia.

Dane użytkownika mogą być przesyłane do aplikacji sieciowej metodami GET lub POST, z użyciem plików cookies lub zmiennych środowiskowych (zawierających informacje o użytkowniku korzystającym ze strony WWW, które można zmodyfikować). Wszystkie te sposoby są podatne na różnego typu ataki SQL Injection. W metodzie GET szkodliwy kod można przekazać w adresie URL (*Uniform Resource Language*), w metodzie POST zaś przez formularz znajdujący się na stronie internetowej.

Do najczęściej występujących ataków SQL Injection należą:

- wstrzyknięcie wyrażenia logicznego o wartości *true*,
- wstrzyknięcie nieprawidłowego zapytania (spreparowane błędy mogą dotyczyć składni zapytania lub nieprawidłowego typowania danych),

- ataki wykorzystujące zapytania z zastosowaniem operatora UNION,
- wstrzyknięcie dowolnego zapytania z wykorzystaniem znaku średnika, który w języku SQL jest separatorem między kolejnymi zapytaniami,
- ataki ślepe umożliwiające sprawdzanie podatności aplikacji, gdy nie wyświetla ona komunikatów o błędzie,
- ataki czasowe (rodzaj ataku ślepego),
- ataki stosujące alternatywny zapis wyrażeń SQL (dla ominięcia podstawowych zabezpieczeń, takich jak filtrowanie znaków specjalnych czy słów kluczowych języka SQL).

Tworzenie spreparowanych zapytań w SQL jest niemal nieograniczone. Ponadto, stosunkowo łatwo można zautomatyzować skanowanie stron internetowych w poszukiwaniu podatności na ten rodzaj ataku, dlatego prawdopodobnie SQL Injection pozostanie nadal jedną z głównych metod atakowania aplikacji sieciowych.

Użytkownicy usług internetowych są bardzo podatni na phishing, czyli ataki o charakterze socjotechnicznym, które polegają na podejmowaniu prób nakłonienia użytkownika do podjęcia określonych, pożądanych przez atakującego działań (np. ujawnienia danych, instalacji szkodliwego oprogramowania). Typowe sposoby stosowane w phishingu to: informowanie o utracie danych lub zagrożeniu systemu, proponowanie korzyści i zastraszanie. Wysyłane wiadomości mogą mieć charakter niespersonalizowany lub spersonalizowany (z wykorzystaniem wcześniej zebranych informacji na temat osoby atakowanej, przez co są bardziej wiarygodne, zatem skuteczniejsze). Charakteryzują je takie cechy jak prośba o otwarcie załącznika, kliknięcie podanego linku do strony WWW, przesłanie wiadomości pod wskazany adres e-mail. Nie dość ostrożni użytkownicy kierowani są na fałszywe strony internetowe zawierające np. formularze, przez które sami mogą przekazać poufne dane lub też nieświadomie pobrać szkodliwy kod. Od 2010 r. liczba rejestrowanych ataków typu phishing wzrosła (w 2012 r. przekroczyła wartość 200 tys.[13]), natomiast czas istnienia stron WWW, z których dokonywane są wyłudzenia, w ostatnich latach spada (w 2012 r. wyniósł średnio ok. 24 godzin), co utrudnia ich wykrywalność. Według przewidywań, zagrożenie, jakim jest phishing spersonalizowany, będzie narastać, gdyż sprzyja temu popularność serwisów społecznościowych – źródło informacji o użytkownikach.

[13] *Global Phishing Survey: Trends and Domain Name Use in 2H2012*, docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf (data odczytu 25.10.2013).

Ze zdalnie przejętych (wskutek infekcji) komputerów tworzone są sieci zwane botnetami, które mogą być używane (w sposób zautomatyzowany) do wielu bezprawnych działań, takich jak atak odmowy dostępu do zasobów i usług (DDoS – *Distributed Denial of Service*), szpiegowanie i pobieranie poufnych danych, hostowanie fałszywych stron internetowych, przechowywanie i udostępnianie nielegalnych plików, ataki *brute force* na systemy kryptograficzne czy rozsyłanie spamu.

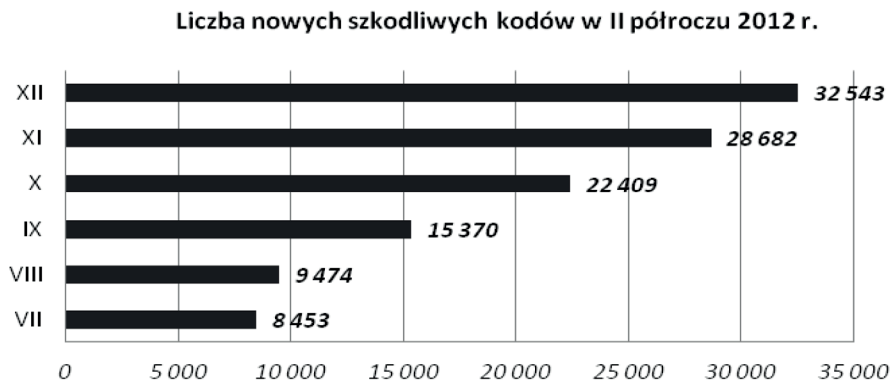
W ostatnich latach w centrum uwagi przestępców sieciowych są urządzenia mobilne będące w pełni funkcjonalnymi komputerami, które są coraz powszechniej używane do realizacji usług z wykorzystaniem Internetu[14]. Z raportu firmy G Data SecurityLabs za 2012 r. wynika, że w stosunku do lat ubiegłych obserwuje się spowolnienie tempa wzrostu zagrożeń dla systemu operacyjnego Windows. W tym samym czasie odnotowano jednak znaczący ich przyrost w przypadku systemu Android – najpopularniejszej platformy systemowej wśród mobilnych systemów operacyjnych (64% udziału). Wzrost nowych szkodliwych kodów dla systemów z oprogramowaniem Android wykrytych w okresie lipiec–grudzień 2012 r. przedstawiono na rysunku 2.

W 2012 r. pojawił się pierwszy botnet złożony z urządzeń mobilnych, działających pod kontrolą systemu Android, zainfekowanych koniem trojańskim dołączonym do nielegalnych wersji popularnych gier i aplikacji[15]. Powstawanie tego typu botnetów jest konsekwencją rozbudowy ich funkcjonalności oraz coraz większej popularności urządzeń mobilnych (głównie smarfonów i tabletów). Z raportu firmy Kindsight, monitorującej stan bezpieczeństwa sieciowego, wynika, że sześć spośród siedmiu najczęściej notowanych typów szkodliwego oprogramowania wykazuje cechy bota (programu do tworzenia sieci z przejętych komputerów i sterowania nimi)[16].

[14] *G Data Malware Report*, gdatasoftware.co.uk/uploads/media/GData_MWR_H2_2012_EN_01.pdf (data odczytu 25.10.2013).

[15] www.symantec.com/connect/blogs/mdk-largest-mobile-botnet-china (data odczytu 5.11.2013).

[16] www.kindsight.net/sites/default/files/Kindsight_Security_Labs-Q412_Malware_Report--final.pdf (data odczytu 25.10.2013).



Rysunek 2. Liczba nowego szkodliwego oprogramowania dla systemu Android wykrytego w drugim półroczu 2012 r. przez G Data SecurityLabs

Źródło: opracowanie własne na podstawie *G Data Malware Report*.

Włamania do systemów i nielegalne pozyskiwanie danych odnotowują zarówno małe, jak i bardzo duże, dobrze zabezpieczone firmy, a także użytkownicy indywidualni. W 2009 r. miała miejsce kradzież danych 160 mln kart płatniczych z pięciu firm, m.in. z Heartland Payment Systems, 7-Eleven i Hannaford Brothers[17]. Do przeprowadzenia ataków wykorzystano szkodliwe oprogramowanie oraz podatność na atak SQL Injection. Dzięki tej metodzie wcześniej uzyskano dostęp do baz danych systemu handlu akcjami NASDAQ (*National Association of Securities Dealers Automated Quotations*). Duże straty wskutek wycieku danych klientów poniosła firma Sony po serii włamań w 2011 r. do PlayStation Network[18]. Brytyjskie Biuro Informacji Publicznej uznało, że bezpieczeństwo kart płatniczych i dane użytkowników wykorzystywane do logowania powinny mieć najwyższy priorytet i wymierzono firmie karę 250 tys. funtów[19]. W 2012 r. w Holandii w wyniku ataku do Internetu trafiły dane prawie 500 tys. pacjentów, a w Utah (USA) wykradziono dane (nazwiska, numery ubezpieczeń oraz inne informacje dotyczące pacjentów) co najmniej 9% z 260 tys. osób zarejestrowa-

[17] www.theafricanworld.tv/2013/07/26/usa-five-russians-ukrainians-indicted-for-compromising-160-million-payment-cards (data odczytu 25.10.2013).

[18] L. Krakowiak, *Kolejny cios w Sony, znów wyciek danych*, 4.05.2011, pcworld.pl/news/369813/ Kolejny.cios.w.Sony.znow.wyciek.danych.html (data odczytu 25.10.2013).

[19] www.ico.org.uk/news/latest_news/2013/ico-news-release-2013 (data odczytu 24.01.2013).

nych w Departamencie Zdrowia[20]. W październiku 2013 r. z bazy amerykańskiego przedsiębiorstwa Adobe Systems[21] wyciekły dane 38 mln klientów (hasła i numery kart płatniczych).

Także w Polsce niejednokrotnie dochodziło do kradzieży poufnych danych. W 2013 r. odnotowano liczne przypadki przechwytywania haseł do internetowych kont bankowych z wykorzystaniem koni trojańskich Citadel i Zitmo[22]. Zainfekowanie komputera koniem trojańskim Banapter (np. przesyłanym w załącznikach do e-maili o niezapłaconej fakturze VAT) skutkuje zamianą numeru rachunku (w przypadku jego kopiowania) podczas wykonywania internetowych przelewów bankowych.

Podobnych przykładów można podać więcej, wszystkie wskazują, że problem zagrożeń jest aktualny i nie można go bagatelizować. Dla bezpieczeństwa, każdy użytkownik sieci powinien właściwie skonfigurować swój system, korzystając z ustawień prywatności, zrezygnować z zapisu haseł dostępowych (do serwisów społecznościowych, aukcyjnych, sklepów, banków itp.) w przeglądarce internetowej i kliencie pocztowym oraz zawsze na zakończenie działalności zakończyć poprawnie sesję.

Aplikacje internetowe przed ich wdrożeniem powinny być zawsze dokładnie przetestowane w środowisku odpowiadającym warunkom ich użytkowania. Do przeprowadzania testów penetracyjnych aplikacji sieciowych służą specjalnie opracowane metodyki, techniki i narzędzia. Dla utrudnienia przeprowadzenia ataku wykorzystującego błędy programowe twórcy systemów operacyjnych zaczęli w nich implementować technologie zapobiegające wykorzystaniu wykrytej podatności do wykonania szkodliwego kodu, takie jak ASLR (*Adresse Space Layout Randomization*) oraz DEP (*Data Execution Prevention*). W celu podniesienia poziomu ochrony wskazane jest zainstalowanie aplikacji filtrującej żądania HTTP na podstawie zdefiniowanych reguł – dzięki zaporom kontrolującym dane wejściowe i wyjściowe aplikacji internetowych (jak np. Modsecurity czy Cloudflare) można uniknąć klasycznych ataków typu XSS lub SQL Injection[23].

[20] www.niszczenie.pl/nowosci/dane-osobowe-w-ochronie-zdrowia-i-badaniach-klinicznych-vii-europejski-dzien-ochrony-danych (data odczytu 28.01.2013).

[21] www.reuters.com/article/2013/11/07/us-adobe-cyberattack-idUSBRE9A61D220131107 (data odczytu 7.11.2013).

[22] zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-trojan-citadel (data odczytu 12.11.2013).

[23] www.owasp.org/index.php/Web_Application_Firewall (data odczytu 5.11.2013).

4. Wybrane aspekty prawne usług elektronicznych

Podmioty oferujące usługi elektroniczne powinny udostępniać użytkownikom warunki ochrony danych. Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych usług (Dz. U. z 2012 r. Nr 0, poz. 1445) nakłada na usługodawcę obowiązek zawarcia w umowie z klientem informacji o podejmowanych działaniach dotyczących zaobserwowanych naruszeń bezpieczeństwa. Ponadto, od 22 marca 2013 r. właściciele witryn internetowych muszą uzyskać zgodę od użytkownika strony WWW na tworzenie plików cookies na jego urządzeniu.

Zgodnie z art. 12 ustawy o świadczeniu usług drogą elektroniczną, odpowiedzialności za bezprawne działania dokonane przez użytkowników nie ponosi podmiot świadczący usługi przekazu danych, jeśli nie jest on inicjatorem tego przekazu. Wyłączenie od odpowiedzialności dotyczy także usługodawców udostępniających zasoby serwerów, jeśli dane pozostają w systemie jedynie na czas transmisji.

W Unii Europejskiej oraz w Stanach Zjednoczonych obowiązują różne przepisy i wymagania odnośnie do ochrony danych osobowych. Aby umożliwić współpracę podmiotów z różnych krajów, a jednocześnie zagwarantować właściwy poziom bezpieczeństwa transferowanych danych osobowych, Unia Europejska (decyzją Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r.) wprowadziła program *Safe Harbour*, przyznający certyfikaty podmiotom z USA, jeśli spełniają europejskie wymogi odnośnie do ochrony danych. Dużym problemem dla dostawców usług świadczonych drogą elektroniczną są nadużycia dokonywane przez użytkowników (takie jak naruszanie praw autorskich, umieszczanie w sieci obraźliwych wpisów i fałszywych informacji). Program *Safe Harbour* umożliwia wyłączenie dostawców usług od odpowiedzialności za tego typu incydenty, jeśli zadeklarują przestrzeganie zasady *notice and take down*.

Portale internetowe, w szczególności strony administracji publicznej, powinny być dostosowywane do potrzeb osób niepełnosprawnych, co jest przedmiotem starań organizacji W3C (World Wide Web Consortium), zajmującej się ustanawianiem standardów tworzenia i przesyłania stron WWW. Zainicjowana przez nią działalność w tym kierunku – WAI (*Web Accessibility Initiative*) – zaowocowała wydaniem standardu WCAG 2.0 (*Web Content Accessibility Guidelines*), dotyczącego tworzenia i dostępności stron internetowych. Dostawcy usług elektronicznych powinni stosować się do zawartych w nim wytycznych. Od czerwca 2015 r. standardy WCAG 2.0 będą obowiązkowe także w przypadku polskich serwisów

administracji publicznej, zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Obecnie w Unii Europejskiej trwają prace nad nowym rozporządzeniem o ochronie danych osobowych, jednolitym dla wszystkich państw członkowskich, uwzględniającym nowe formy komunikacji i przetwarzania danych. Wiele danych z pozoru nieistotnych nabiera – ze względu na ich dostępność i możliwość łączenia – znaczenia i może być traktowanych jako dane umożliwiające jednoznaczną identyfikację osoby. W październiku 2013 r. Ministerstwo Administracji i Cyfryzacji przyłączyło się do programu *Partnerstwo dla zwiększenia świadomości obywateli na temat cyfrowej tożsamości*.

Systemy teleinformatyczne wykorzystywane przez różne podmioty (np. służby specjalne) podlegają różnym wymaganiom i ograniczeniom. Paragraf 15 rozporządzenia Ministerstwa Spraw Wewnętrznych z 31 grudnia 2012 r. określa sposoby przetwarzania danych, takie jak: rejestrowanie, sprawdzanie, klasyfikowanie, weryfikowanie, modyfikowanie, typowanie, analizowanie, przekazywanie, usuwanie i wykorzystywanie. Wszystkie wykonywane czynności muszą być rejestrowane przez system lub administratora danych: data i czas rozpoczęcia i zakończenia pracy, identyfikacja pracownika i zlecającego, zakres informacji, data pierwszego wprowadzenia danych, źródło informacji, cel i przyczyna wykonania operacji, a także przyczyny, zakres i cel modyfikacji danych oraz wnioski z wykonywanych czynności. Specyficzne przepisy obowiązują np. w jednostkach administracji publicznej[24] oraz w ochronie zdrowia[25].

W ostatnich latach wraz z rozwojem usług świadczonych drogą elektroniczną obserwuje się powstawanie stosownych przepisów i aktów prawnych. Od 4 sierpnia 2005 r. faktury elektroniczne zabezpieczone podpisem cyfrowym są traktowane przez polskie prawo na równi z fakturami w wersji papierowej. Wiele firm coraz częściej wykorzystuje usługę poczty elektronicznej do przesyłania takich dokumentów swoim klientom. Szacuje się, że w Europie około 15% faktur jest wystawianych w postaci elektronicznej. Obecnie trwają prace nad wprowadzeniem dyrektywy dotyczącej faktur elektronicznych w krajach członkowskich Unii Europejskiej i opracowaniem dla nich jednolitego standardu. W ramach

[24] T. Burczyński, *Elektroniczna wymiana informacji w administracji publicznej*, PRESSCOM, Wrocław 2011.

[25] K. Nyczaj, P. Piecuch, *Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej*, Wiedza i Praktyka, wyd. 3, Warszawa 2013.

polityki spójności realizowanej w latach 2014–2020 zakłada się cyfryzację Polski (m.in. szerokopasmowy dostęp do Internetu oraz rozwój e-usług w administracji) oraz cyfryzację procesów zakupowych we wszystkich państwach unijnych.

Mimo bogatej oferty usług elektronicznych oraz wygody i szybkości ich realizacji, wiele osób świadomie ogranicza korzystanie z nich z obawy o bezpieczeństwo transakcji finansowych oraz konieczność udostępniania danych osobowych.

5. Podsumowanie

Z uwagi na skalę realnych zagrożeń dynamiczny rozwój usług świadczonych drogą elektroniczną wymaga zapewnienia optymalnego poziomu ich ochrony. W tym celu oferowane standardy bezpieczeństwa powinny być użytkowane z wykorzystaniem najmocniejszych dostępnych mechanizmów. W przypadku wielu zastosowań widoczna jest potrzeba wprowadzenia nowych, lepszych rozwiązań, dostosowanych do obecnych problemów.

Istnieje też konieczność modyfikacji istniejących i szybkiego opracowania nowych przepisów oraz uregulowań prawnych, odpowiadających wymogom rozwijającej się gospodarki elektronicznej. Dostępne urządzenia i oprogramowanie umożliwiające niezauważalne monitorowanie wszelkiej aktywności sieciowej dodatkowo wymuszają tę potrzebę. Ważne jest to, by tworzone dokumenty zawierały definicje nowo tworzonych pojęć, by były spójne i nie wprowadzały luk umożliwiających dowolną interpretację przepisów – choć wydaje się to oczywiste, w praktyce nie zawsze jest osiągane. Od poziomu ochrony usług świadczonych drogą elektroniczną zależy zaufanie do nowoczesnych technologii, a tym samym ich powszechne użytkowanie i dalszy rozwój.

Bibliografia

1. Adamski D., Litwiński P., Martysz C., Okoń Z., Sibiga G., Szostak R., Szostek D., Świerczyński M., *E-administracja. Prawne zagadnienia informatyzacji administracji*, PRESSCOM, Wrocław 2009.
2. Burczyński T., *Elektroniczna wymiana informacji w administracji publicznej*, PRESSCOM, Wrocław 2011.

3. Nyczaj K., Piecuch P., *Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej*, Wiedza i Praktyka, Warszawa 2013.
4. Pręda B., *Wyłączenie odpowiedzialności za udostępnianie linków – uwagi do projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną*, „Kwartalnik Naukowy: Prawo Mediów Elektronicznych" 2012, nr 2.
5. Rozporządzenie 2006/1987/WE Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
7. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204).
8. Ustawa z dnia 7 listopada 2008 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną (Dz. U. z 2008 r. Nr 216, poz. 1371).
9. Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. z 2012 r. Nr 0, poz. 1445).
10. Ustawa z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. z 2013 r. Nr 0, poz. 1036).

Źródła sieciowe

1. *Dane osobowe w ochronie zdrowia i badaniach klinicznych – VII Europejski Dzień Ochrony Danych Osobowych*, www.niszczenie.pl/nowosci/dane-osobowe-w-ochronie-zdrowia-i-badaniach-klinicznych-vii-europejski-dzien-ochrony-danych (data odczytu 28.01.2013).
2. Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych, p1.csioz.gov.pl (data odczytu 5.11.2013).
3. *Find out how many vulnerabilities were discovered in 2012*, http://secunia.com/vulnerability-review/vulnerability_update_all.html (data odczytu 5.11.2013).
4. Finkle J., *Trove of Adobe user data found on Web after breach: security firm*, www.reuters.com/article/2013/11/07/us-adobe-cyberattack-idUSBRE9A61D2201 31107 (data odczytu 7.11.2013).
5. *G Data Malware Report*, gdatasoftware.co.uk/uploads/media/GData_MWR_H2_2012_EN_01.pdf (data odczytu 25.10.2013).
6. *Global Phishing Survey: Trends and Domain Name Use in 2H2012*, docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf (data odczytu 25.10.2013).
7. Internetowy System Aktów Prawnych, isap.sejm.gov.pl (data dostępu 5.11.2013).

8. *Komisja zapowiada wsparcie w wysokości 13,7 mln euro na transgraniczne cyfrowe usługi publiczne*, komunikat prasowy Komisji Europejskiej: europa.eu/rapid/press-release_IP-13-778_pl.htm (data odczytu 5.11.2013).
9. Krakowiak L., *Kolejny cios w Sony, znów wyciek danych*, 4.05.2011, pcworld.pl/news/369813/Kolejny.cios.w.Sony.znow.wyciek.danych.html (data odczytu 25.10.2013).
10. *Malware Report Q4 2012*, www.kindsight.net/sites/default/files/Kindsight_ Security_Labs-Q412_Malware_ Report-final.pdf (data odczytu 25.10.2013).
11. *MDK: The Largest Mobile Botnet in China*, www.symantec.com/connect/blogs/mdk-largest-mobile-botnet-china (data odczytu 5.11.2013).
12. *OWASP Testing Project*, www.owasp.org/index.php/OWASP_Testing_Project (data odczytu 5.11.2013).
13. *Rejestry medyczne. Wszystko o projekcie P2*, http://wartowiedziec.org/index.php/ zdrowie/zarzadzanie/10232-wszystko-o-projekcie-p2 (data odczytu: 25.10.2013).
14. *Sony fined £250,000 after millions of UK gamers' details compromised*, www.ico.org.uk/news/latest_news/2013/ico-news-release-2013 (data odczytu 24.01.2013).
15. *Top 10 2013*, owasp.org/index.php/Top_10_2013 (data odczytu 5.11.2013).
16. *Trojan Citadel atakuje PC – Trojan Zitmo infekuje telefony komórkowe*, Komunikat z dnia 24 kwietnia 2013 r., zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-trojan-citadel (data odczytu 12.11.2013).
17. *USA: Five Russians, Ukrainians indicted for compromising 160 million payment cards*, www.theafricanworld.tv/2013/07/26/usa-five-russians-ukrainians--indicted-for-compromising-160-million-payment-cards (data odczytu 25.10.2013).
18. *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, nr ewid. 107/2013/P/12/191/KPB – wersja jawna, bip.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole, 11898.html (data odczytu 5.11.2013).
19. *Web Application Firewall*, www.owasp.org/index.php/Web_Application_Firewall (data odczytu 5.11.2013).
20. Zintegrowany Informator Pacjenta, zip.nfz.gov.pl (data odczytu 5.11.2013).

* * *

Electronic services in the context of threats

Summary

In the era of rapid development of electronic commerce, almost every organisation (an institution, company, or firm) uses in its work an IT system, collecting and processing data which can also be transferred at a distance as part of the services the

organisation provides. The clients (petitioners) are increasingly often able to do many things remotely using the constantly expanding Internet. Unfortunately, running services over the network is exposed to various risks. IT systems can in fact be successfully attacked, which may have consequences such as unauthorised access to data or taking control over the system. The reasons of such adverse events are primarily defects and improper configuration of the software in use. This article presents the dynamics of development of electronic services primarily in the public administration and health care, it raises a number of issues related to their implementation and discusses some legal aspects thereof. Due to the gravity and extent of the phenomenon, particular attention has been given to network-related threats.

Keywords: data security, electronic services