Halina Świeboda[1]
Paweł Stobiecki[2]

Bezpieczeństwo urządzeń mobilnych w przestrzeni cyfrowej

Wprowadzenie

Dynamiczna cyfrowa transformacja jest przykładem coraz szerszej absorbcji technologii informatycznych obserwowanej dzięki jej zastosowaniu w różnych obszarach aktywności i działalności społecznej. Ilość usług w cyberprzestrzeni stale się zwiększa. Wdrażane są różnego rodzaju platformy informatyczne i udostępniane są usługi e-administracji, e-zdrowia, e-edukacji, e-biznesu. Coraz chętniej wykorzystywane są do prowadzenia tego typu działalności urządzenia mobilne. Bardzo często na urządzeniach mobilnych przechowuje się nie tylko dane prywatne, ale również służbowe. Wyciek poufnych informacji z firmy czy przedsiębiorstwa jest bardzo niebezpiecznym zjawiskiem, ale użytkownicy często nie zdają sobie sprawy z zagrożeń. Praktyka dostarcza coraz to nowych przykładów jak bezpieczeństwo i jego poczucie bywa zwodnicze.

E-usługi podstawą nowoczesnego i innowacyjnego państwa

Świadczenie usług w Internecie uznaje się za efekt innowacji związanych z rozwojem technologii informatycznych. Innowacje tego typu dotyczą[3]:
— nowego kanału świadczenia usługi wcześniej realizowanej w tradycyjny sposób, rozumianego jako komplementarny, a nie substytucyjny element procesu usługowego;

[1] Dr hab. Halina Świeboda — prof. ASzWoj, kierownik Katedry Bezpieczeństw Informacyjnego i Komunikacji Instytutu Studiów Strategicznych Wydziału Bezpieczeństwa Narodowego w Akademii Sztuki Wojennej.

Adres do korespondencji: <h.swieboda@akademia.mil.pl>.

[2] Dr Paweł Stobiecki — adiunkt w Katedrze Bezpieczeństwa Informacyjnego i Komunikacji Instytutu Studiów Strategicznych Wydziału Bezpieczeństwa Narodowego w Akademii Sztuki Wojennej.

Adres do korespondencji: <p.stobiecki@akademia.mil.pl>.

[3] R. Wolny, *Rynek e-usług w Polsce — funkcjonowanie i kierunki rozwoju,* Katowice 2013, s. 14.

— nowego sposobu dystrybuowania informacji;
— nowej formy handlu w postaci rynków cybernetycznych i aukcji internetowych;
— nowych kanałów rozprzestrzeniania informacji o usługach (SMS, e-mail, katalogi i instrukcje on-line);
— szybszych sposób uaktualniania usługi;
— nowego sposobu pośrednictwa na wielu rynkach, przy czym miejscem spotkania zainteresowanych stron nie jest rynek w rozumieniu geograficznym, lecz Internet[4].

E-usługi to forma świadczenia usług przy wykorzystaniu Internetu, zawierająca w szczególności prezentację usługi, zamówienie, zapłatę oraz korzystanie z usługi przez Internet, z zastrzeżeniem, że w przypadku wybranych usług korzystanie z nich (konsumpcja) odbywa się w świecie rzeczywistym (niewirtualnym). Usługi różnią się od dóbr zawartością komponentów materialnych. Dotyczy to również e-usług, które — podobnie jak usługi tradycyjne — charakteryzują się specyficznymi cechami, które pozwalają na wykonywanie czynności w cyberprzestrzeni (tabela 1).

Tabela 1

Charakterystyka wybranych e-usług

E-usługi	Przykłady czynności dokonywanych w Internecie
e-administracja	pobieranie i składanie formularzy, pozyskiwanie informacji, rozliczenie podatku
e-bankowość	otwieranie rachunków i lokat, zaciąganie kredytów, dokonywanie przelewów, spłata kredytów i kart kredytowych
e-edukacja	nauka na kursach i szkoleniach tematycznych, nauka języka, studiowanie na studiach licencjackich, studiowanie na studiach magisterskich, studiowanie na studiach podyplomowych
e-handel	sprzedawanie towarów, kupowanie towarów, porównywanie cen
e-kultura	zwiedzanie wirtualnego muzeum i galerii, oglądanie filmów i spektakli, czytanie i słuchanie książek, czytanie gazet i czasopism, słuchanie radia, oglądanie telewizji, słuchanie muzyki, oglądanie wideoklipów, sprawdzanie repertuaru, kupowanie biletów
e-turystyka	kupowanie wycieczek, rezerwacja miejsc noclegowych, odprawa *on-line,* kupowanie biletów autobusowych, kolejowych i lotniczych
e-ubezpieczenia	obliczanie składki ubezpieczenia, zakup ubezpieczeń, zgłaszanie szkody, pozyskiwanie informacji o odszkodowaniu
e-zdrowie	wyszukiwanie informacji dotyczących profilaktyki zdrowotnej, sprzedawanie leków, sprzedawanie sprzętu medycznego, monitorowanie stanu zdrowia, wyszukiwanie lekarzy specjalistów oraz przychodni i poradni, zapisy na wizyty

Źródło: R. Wolny, *Rynek e-usług w Polsce — funkcjonowanie i kierunki rozwoju*, Katowice 2013, s. 23

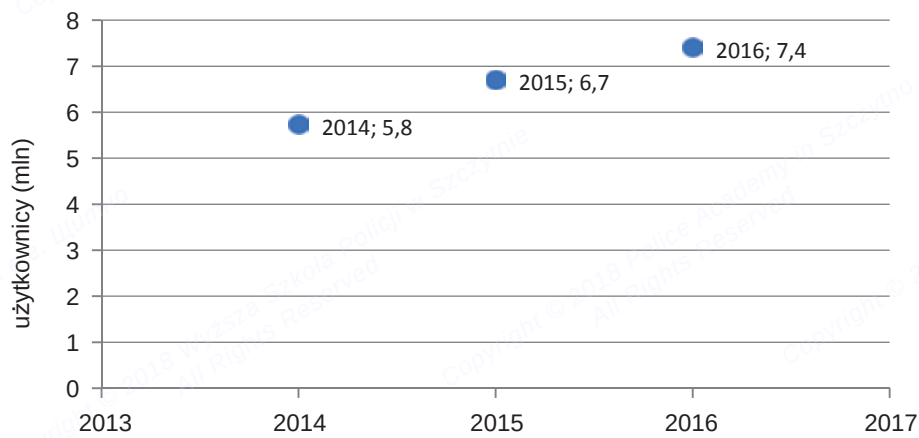
[4] I. Rudawska (red.), *Usługi w gospodarce rynkowej,* Warszawa 2009, s. 158.

E-usługi należą do teleinformatycznej infrastruktury krytycznej. W tym szczególnie ważny pozostaje segment bankowości i finansów, kluczowy z punktu widzenia funkcjonowania państwa, społeczeństwa, przedsiębiorców i obywateli. Dostępność i bezpieczeństwo segmentu ma wpływ na jego stabilność, co przekłada się w pewnej części na bezpieczeństwo ekonomiczne.

Do realizacji usług coraz chętniej wykorzystywane są urządzenia mobilne. Wzrasta liczba użytkowników Internetu mobilnego (wykres 1). W 2016 r. 7,86 mln osób korzystało z usług wiązanych, liczba użytkowników tego typu wzrosła o 34% w porównaniu do roku poprzedniego. Modele prognostyczne wskazują na dalszą eskalację trendu. Najpopularniejszą usługą wiązaną niezmiennie pozostaje pakiet „Telefonia ruchoma + Internet mobilny". Użytkownicy tej usługi stanowili 54% wszystkich abonentów, co oznaczało wzrost o ponad 12,5 punktów procentowych. w porównaniu do roku 2015[5]. Można szacować, że całkowity wkład telefonii mobilnej w Polskie PKB wynosi około 3,2%[6].

Wykres 1

Liczba abonentów Internetu mobilnego w mln



Źródło: Opracowanie własne na podstawie danych UKE

Rynek systemów, pod kontrolą których pracują urządzenia mobilne, zdominowany jest przez platformę Android firmy Google, przeznaczoną dla smartfonów, telefonów komórkowych, tabletów i netbooków, okazuje się bowiem, że 85% urządzeń mobilnych pracuje pod kontrolą tego systemu. Drugim popularnym systemem dla urządzeń mobilnych, takich jak iPhone'y, iPody touche oraz iPady, jest system operacyjny iOS Apple Inc.

[5] UKE, *Raport o stanie rynku telekomunikacyjnego w 2016 roku*, Warszawa 2017.

[6] PwC, *Technologie mobilne w nowoczesnej Polsce — odpowiedzialny rozwój i równe szanse,* październik 2016 r., <https://www.pwc.pl/pl/pdf/technologie-mobilne-raport-pwc.pdf>, 12 grudnia 2018 r.

Ale jego udział w rynku urządzeń mobilnych to tylko 14,3%[7]. Pozostałe systemy, takie jak Windows Phone, Java ME czy Symbian, Black Berry, Samsung, wypełniają pozostałą cześć rynku, póki co, nie stanowiąc konkurencji dla platformy Android i iOS.

Android oparty na systemie operacyjnym Linuxa niestety w kwestii bezpieczeństwa ustępuje platformie iOS urządzeń iPhone firmy Apple, ale w każdej kolejnej wersji wprowadzane są coraz lepsze zabezpieczenia. Jakość i niezawodność urządzeń, jak i liczba oferowanych usług ciągle wzrasta. Niestety doskonaleniu technologii bezpieczeństwa towarzyszy rozwój technologii wykorzystywanych do popełniania cyberprzestępstw.

Według Open Web Application Security Project (OWASP)[8] wśród aktualnych zagrożeń dla aplikacji mobilnych znalazły się między innymi:
— słabe mechanizmy zabezpieczeń procesów autoryzacji i uwierzytelniania,
— niewystarczająca ochrona warstwy transportowej,
— niezabezpieczenie komponentów IPC,
— możliwość wstrzykiwania danych po stronie klienta,
— modyfikacji aplikacji po uzyskaniu dostępu do jej kodu źródłowego.

Straty z powodu znacznej liczby incydentów naruszających bezpieczeństwo cybernetyczne w USA wynikające z godziny przestoju całego sektora w instytucjach finansowych wynoszą 1,4 mln dol., natomiast w bankowości 996 tys. dol.[9] Potencjalne straty sektora finansowego w Polsce to około 1 mld zł[10].

Urządzania mobilne nie są w pełni bezpieczne, stąd pojawia się pytanie — na ile bezpieczne jest realizowanie usług płatności mobilnych, skądinąd tak istotnych zarówno dla obywatela, jak i państwa?

Niebezpieczne płatności mobilne

Przez bankowość mobilną, nazywaną po angielsku *mobile banking* lub *m-banking*, rozumie się zestaw narzędzi, które za pomocą telefonu lub innego urządzenia mobilnego z dostępem do Internetu (np. telefonu czy tabletu) umożliwiają korzystanie z usług bankowych poprzez dedykowaną aplikację mobilną lub mobilny serwis WWW.

Usługa bankowości internetowej jest regulowana na mocy ustawy o elektronicznych instrumentach płatniczych, która zobowiązuje bank do „zapewnienia dostępu do środków pieniężnych zgromadzonych na rachunku za pośrednictwem urządzeń łączności przewodowej lub

[7] IDC Worldwide Quarterly Mobile Phone Tracker, November 29, 2016.

[8] Firma jest globalną fundacją zajmująca się zabezpieczeniami sieciowymi.

[9] IT Performance Engineering & Measurement Strategies: Quantifying Performance Loss, Meta Group, October 2000, <http://www.bitway.biz/en/what-why-how.aspx>, 12 stycznia 2018 r.

[10] J. Ramotowski, *Potencjalne straty sektora finansowego to 1 mld zł*, wywiad z P. Skowronem z firmy White Cat Security zajmującej się wzmacnianiem elektronicznej obrony, <https://www.obserwatorfinansowy.pl/tematyka/bankowosc/potencjalne-straty-sektora-finansowego-to-1-mld-zl/>, 19 lutego 2018 r.

bezprzewodowej wykorzystywanych przez posiadacza, a także do wykonywania operacji lub innych czynności zleconych przez posiadacza”[11]. Banki za pośrednictwem telefonu komórkowego oferują m.in.:
— sprawdzenie stanu konta,
— sprawdzenie historii operacji,
— dokonanie przelewu,
— sprawdzenie listy rabatów związanych z płatnością kartą,
— otworzenie lokaty,
— spłaty karty,
— znalezienie najbliższego bankomatu w okolicy.

W Polsce od lat działają usługi IKO Banku PKO BP i Peopay Banku Pekao S.A., które są jednymi z większych wdrożeń w Europie. Jednocześnie w ramach współpracy w zakresie płatności mobilnych 7 banków (Alior Bank, Bank Millennium, Bank Zachodni WBK, ING Bank Śląski, mBank, Getin Bank oraz PKO Bank Polski) założyło Polski Standard Płatności, wyznaczając tym samym międzybankowy standard płatności mobilnych. Trzeba podkreślić, że rozwiązanie problemu płatności mobilnych, w dłuższym okresie, w istotny sposób wpłynie na obrót gotówką oraz użycie kart płatniczych, wyznaczając również standard bezpieczeństwa.

W związku z faktem, że przesyłane dane są na linii nadawca — odbiorca przechodzą one przez liczne sieci komputerowe. Wówczas pojawia się ryzyko ingerencji ze strony osób trzecich, a to w konsekwencji może prowadzić do przypadków narażających integralność danych na:
— przerwanie transmisji danych,
— przechwycenie przesyłanych informacji,
— ich podrobienie.

Wystąpienie tego rodzaju incydentów naraża zarówno klienta, jak i bank na straty finansowe. Uzyskanie danych przez osoby postronne może zostać wykorzystane do nielegalnych czynności prowadzących do utraty środków przez klienta. Przerwanie transmisji lub zmiana zawartości przesyłanych danych z kolei może prowadzić do zmiany pakietów informacji przesyłanych między użytkownikiem a systemem bankowości internetowej. Ta sytuacja generuje ryzyko utraty integralności informacji. Taka okoliczność może zdarzyć się wtedy, kiedy atakujący przejmie kontrolę nad telefonem ofiary, która korzysta z aplikacji mobilnej, logując się do banku. Biorąc pod uwagę fakt, iż telefon jest jedynym narzędziem uwierzytelniającym w takim przypadku, istnieje możliwość podmiany konta oraz kwoty przesyłanej w ramach transferów pieniężnych.

Dynamiczny rozwój nowych technologii IT w kwestii ataków hackerskich sprawił, że obok poznanych metod, które jednak ciągle ewoluują, pojawiają się nowe, często trudniejsze do wykrycia. W palecie narzędzi, z których najczęściej korzystają cyberprzestępcy w celu nielegalnej

[11] Ustawa o elektronicznych usługach płatniczych z 2 września 2002 r. (DzU z 2002 r., nr 169, poz. 1385), art. 29.

ingerencji w transmisje danych przez Internet[12] wyróżnić można: sniffing, tampering, spoofing, phishing oraz ransomware.

Zagrożenia stają się bardziej niebezpieczne, ponieważ złośliwe i fałszywe aplikacje mogą się pojawiać na oficjalnych stronach. Dowodzi tego przykład pojawienie się dwóch złośliwych aplikacji CryptoMonitor oraz StorySaver w sklepie Google Play. Sytuacja miała miejsce w listopadzie 2017 r.[13] CryptoMonitor miał służyć do monitorowania cen krytpowalut, natomiast druga z wymienionych aplikacji teoretycznie miała służyć do zapisywania tzw. Stories z Instagrama, czyli krótkich historii użytkownika z ostatniej doby. Obie aplikacje wykonywały zadania, które wynikały z opisów zamieszczonych w Google Play, ale ich ukrytym celem było wykradanie dostępu mobilnego do kont bankowych i okradanie rachunków[14].

Najczęściej stosowane metody w cyberatakach

Sniffing polega na przechwytywaniu i analizowaniu pakietów sieciowych, które docierają do naszych interfejsów sieciowych. Jest to proces określany jako nasłuchiwanie ruchu sieciowego, który pozwala na uzyskanie danych. Metoda ma charakter bierny, nie stanowi bezpośredniego większego zagrożenia, ale jest narzędziem pozwalającym uzyskać niezbędne dane do realizacji innych przestępstw, bardziej niebezpiecznych i stanowiących bezpośrednie zagrożenie[15]. Daje możliwość monitorowania i rejestrowania identyfikatorów i haseł, za pomocą których dochodzi do logowania np. do bankowości internetowej. Realizacja ataku typu sniffing jest możliwa, kiedy atakujący jest w tej samej sieci (np. w sieci wifi), w której znajdują się ofiary. Nasłuchiwanie ruchu sieciowego umożliwia przejęcie loginu i haseł do różnych portali lub aplikacji.

Metoda tampering (inaczej ingerencja osób niepowolanych) polega na przechwyceniu danych oraz ich modyfikacji przez osoby postronne, zaś do odbiorcy docierają informacje o zmienionej treści. Jest to metoda, która stanowi bezpośrednie zagrożenie, ponieważ w momencie dokonywania czynności bankowej włamywacze mogą zmienić parametry danej transakcji, a w tym: numer rachunku np. na własny, tak by przesyłane

[12] Związek Banków Polskich, <https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe>, 19 stycznia 2018 r.

[13] Wintermute, *Atak na polskich użytkowników bankowości mobilnej,* <https://www.chip.pl/2017/12/atak-polskich-uzytkownikow-bankowosci-mobilnej/>, 12 grudnia 2018 r.

[14] Tamże, według ekspertów firmy ESET na celowniku cyberprzestępców znalazły się aplikacje mobilne aż 14 polskich banków: Alior Mobile, BZWBK24 mobile, Getin Mobile, IKO, Moje ING Mobile, Bank Millenium, mBank PL, BusinessPro, Nest Bank, Bank Pekao, PekaoBiznes24, plusbank24, Mobile Bank, Citi Handlowy.

[15] Zob. wykład III. *Zdalne rozpoznawanie systemów operacyjnych i sniffing* <http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index19.html>, 10 stycznia 2018 r.

środki trafiły na ich konto. W konsekwencji może to doprowadzić do strat finansowych dla klienta i banku. Atak typu tampering może być wykonany przy pomocy metod sniffingu, czyli „węszenia w sieci" polegającego na odczytywaniu danych przez węzeł, dla którego nie były one przeznaczone, np. odczytywanie haseł czy numerów kont finansowych. Przy nasłuchiwaniu ruchu sieciowego atakujący ma możliwości przejęcia plików cookies aktualnie zalogowanego użytkownika systemu bankowego. Przejęcie plików cookies, umożliwia uwierzytelnienie się do danego systemu jako legalny użytkownik, co może wygenerować duże straty finansowe dla klienta, kradzież informacji oraz wysokie ryzyko utraty reputacji dla organizacji[16].

Kolejną metoda jest spoofing (maskarada), który polega na podszywaniu się pod inny komputer i fałszowaniu usług oraz protokołów sieciowych w taki sposób, by ofiara ataku nie miała możliwości rozpoznania atakującego. Celem jest oszukanie systemów zabezpieczających. W konsekwencji daje to możliwość włamywaczom na uzyskanie dostępu do zasobów sieci i pozyskania, podobnie jak przy sniffingu, np.: imienia, nazwiska, numerów kart kredytowych, identyfikatora i hasła, które są wykorzystywane przy logowaniu do systemów bankowości internetowej. Spoofing może mieć różne formy[17]: ARP spoofing, DNS spoofing, IP spoofing, Route spoofing, IP spofing, Non-blind i Blind spoofing[18]. Przykładowo IP spoofing polega na podmianie adresu źródłowego adresu IP. Strona atakująca wysyła do swojej ofiary pakiet z fałszowanym źródłowym adresem IP, który wskazuje na realną maszynę, z której standardowo korzysta potencjalna ofiara. Przy modyfikacji pakietu zostaje także zmieniony nagłówek tak, by wyglądał na zaufany. Ostatecznie prowadzi to do znacznych utrudnień w komunikacji sieciowej oraz w wykryciu źródła ataku[19].

Kolejny rodzaj metody to phishing, co oznacza *password harvesting fishing*, czyli „łowienie haseł". Idea działania metody sprowadza się do nakłonienia klienta do ujawnienia tajnych informacji osobowych, haseł oraz danych finansowych, dlatego też jednym z ważniejszych aspektów tej metody jest socjotechnika[20]. Polega to na rozsyłaniu wiadomości za pośrednictwem poczty elektronicznej, które mają na celu przekonać użytkownika do odwiedzenia złośliwych stron internetowych czy pobierania złośliwych załączników.

---

[16] Przemek (sopel) Sobstel, *Sesja użytkownika w PHP — zagrożenia i ochrona,* <http://wortal.php.pl/Wortal/Artykuly/Bezpieczenstwo/Sesja-uzytkownika-w-PHP-zagrozenia-i-ochrona/Session-Hijacking>, 10 stycznia 2018 r.

[17] Zob. wykład III. *Zdalne rozpoznawanie...*, wyd. cyt.

[18] Szerzej: P. Krawaczyński, D. Zelek, *Rodzaje i klasyfikacja włamań oraz ataków internetowych,* <http://faqxp.cba.pl/faq/winxp/wlamania.htm>, 1 stycznia 2018 r.

[19] K. Folga*, Spoofing: sztuka ataku i obrony,* <http://www.computerworld.pl/news/Spoofing-sztuka-ataku-i-obrony,315264.html>, 13 stycznia 2018 r.

[20] G. Weidman, *Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne*, Gliwice 2015, s. 312.

Ataki socjotechniczne stanowią ostatni z etapów działań cyberprzestępców. Pozwalają na wymuszenie pewnych zachowań użytkownika w celu przeprowadzenia skutecznego ataku po stronie klienta. Phishing nie ogranicza się jednak tylko do tej metody. Powszechnie wykorzystywane są inne rozwiązania pozwalające pozyskać tajne informacje od klientów[21]. Są to na przykład keyloggery umożliwiające sprawdzenie, które klawisze z klawiatury komputera były naciskane przez klienta podczas logowania, a także działania polegające na umieszczaniu w plikach graficznych niebezpiecznych kodów. Generalnie phishing bazuje, podobnie jak spoofing, na narzędziach socjotechniki oraz lukach w oprogramowaniu wykorzystywanym przez klienta[22].

Ostatnio bardzo dużym zagrożeniem jest ransomware, które zazwyczaj działa w połączeniu z phishingiem. W tej metodzie nie kradnie się danych użytkownika, ale wymusza płatność okupu, zazwyczaj w dolarach lub bitcoinach. Proces polega na wysyłaniu przez atakującego e-maili do dużej liczby użytkowników, próbując nakłonić ich do wejścia na podstawioną stronę internetową poprzez oferowany link lub nakłonienia do pobrania pliku zawierającego złośliwe oprogramowanie. Plikiem może to być np. fałszywa faktura lub wezwanie do zapłaty. Jeśli ofiara zdecyduje się otworzyć plik, ransomware szyfruje wszystkie otwarte dyski (łącznie z sieciowymi) oraz wyświetla informację o konieczności wpłacenia okupu za odblokowanie szyfrowania. Możliwości odzyskania danych są bardzo ograniczone, ponieważ wymagają specjalistycznych, choć darmowych, narzędzi, które mimo wszystko nie zapewniają 100% skuteczności w swoim działaniu[23]. Najbardziej złośliwe rodziny szyfrujących ransomware to Cryptowall, Critroni i TorLocker.

Praktyczny wymiar zagrożeń: badania własne

Dla potwierdzenia założeń sformułowanych na potrzeby niniejszego artykułu przeprowadzono eksperyment w postaci testu penetracyjnego sieci bezprzewodowej. Test odbył się na sieci bezprzewodowej utworzonej specjalnie w tym celu i miał uświadomić użytkownikom jak ważne jest zmienianie standardowych ustawień bezpieczeństwa urządzeń mobilnych, jakimi są mobilne routery wi-fi.

[21] Związek Banków Polskich, <https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe>, 19 stycznia 2018 r.

[22] *Zagrożenia współczesnej bankowości elektronicznej,* <http://prnews.pl/wiadomosci/zagrozenia-wspolczesnej-bankowosci-elektronicznej-3637323.html>, 13 stycznia 2018 r.

[23] A. Haertle, *Masowa, niezwykle skuteczna kampania ransomware wyłącza całe firmy*, <https://zaufanatrzeciastrona.pl/post/masowa-niezwykle-skuteczna-kampania-ransomware-wylacza-cale-firmy/>, 15 maja 2017 r.; *Czym jest ransomware? Przewodnik zapoznawczy — część I*, <https://bitdefender.pl/czym-jest-ransomware-przewodnik-zapoznawczy-czesc-i>, 12 grudnia 2018 r.

Do przeprowadzenia testu użyto komputera z zainstalowanym systemem operacyjnym Kali Linux oraz telefonu komórkowego z zainstalowanym systemem operacyjnym Kali Linux NetHunter[24]. Aby umożliwić komputerowi komunikację z sieciami bezprzewodowymi, wyposażono go w kartę sieciową bezprzewodową opartą o chipset Atheros AR9271[25], zdolną do wstrzykiwania pakietów danych do audytowanej sieci. Należy zaznaczyć w tym miejscu, że wszystkie dane uzyskane w czasie niniejszego testu zostały zanonimizowane, aby możliwe było ich upublicznienie.

Audytowaną sieć utworzono na bazie mobilnego routera wi-fi dostępnego w ofercie polskich sieci komórkowych. Urządzenie pozostawiono skonfigurowano tak, aby zachować standardowe ustawienia producenta. Wprawdzie standardowo ustawionym protokołem zabezpieczenia sieci bezprzewodowej pozostał WPA2-PSK26, który zdaje się nadal pozostawać najlepszą opcją do wyboru, jednak, poza tym zabezpieczeniem, jedną z domyślnych włączonych opcji był również WPS27 (rozwiązanie pozwalające na łatwe łączenie się urządzeń w sieci za pośrednictwem zdefiniowanego przez producenta 8-cyfrowego kodu PIN). To właśnie obecność tej opcji naraża użytkowników na możliwość przełamania bezpieczeństwa ich sieci, która chociaż zabezpieczona silnym protokołem szyfrującym narażona jest na nieautoryzowane połączenie.

Test rozpoczęto od zeskanowania sieci bezprzewodowych będących w zasięgu komputera i telefonu komórkowego. Skanowanie przeprowadzono za pomocą programu airodump-ng28, który pokazuje w czasie rzeczywistym informacje o sieciach będących w zasięgu. Do najważniejszych informacji, jakie można uzyskać za jego pomocą należą przede wszystkim:

— nazwa sieci,
— MAC adres karty sieciowej urządzenia,
— moc sygnału sieci,
— protokół szyfrujący,
— informacja o zabezpieczeniu sieci,
— podłączeni klienci.

Wyniki skanowania sieci bezprzewodowych zaprezentowano na rysunku 1.

[24] Zob. stronę Internetową Offensive Security, <https://www.kali.org/>, 29 marca 2018 r.

[25] Jeden z chipsetów obsługiwanych przez system operacyjny Kali Linux, który wspiera wstrzykiwanie pakietów danych.

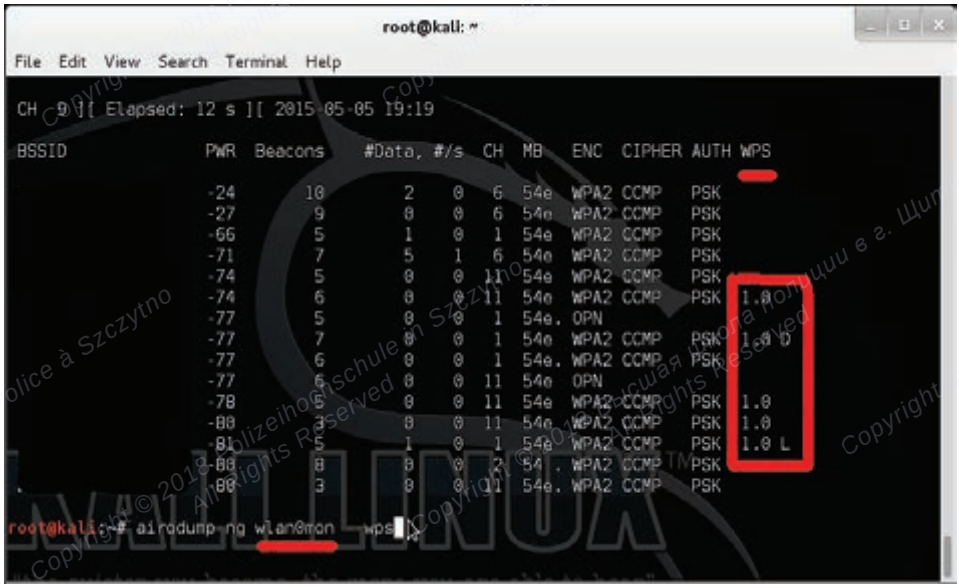
[26] Szyfrowanie Wi-Fi Protected Access w wersji drugiej, połączone z mechanizmem autoryzacji za pomocą hasła Pre-Shared Key.

[27] Wi-Fi Protected Setup.

[28] Zob. stronę Internetową programu airodump-ng, <https://www.aircrack-ng.org/>, 29 marca 2018 r.

Rysunek 1

Wynik wyszukiwania sieci bezprzewodowych



Źródło: opracowanie własne — zrzut ekranu z programu airodump-ng

W wyniku skanowania wykryto między innymi sieci bezprzewodowe zabezpieczone protokołem WPA2-PSK oraz posiadające aktywną funkcję WPS. Tak jak wspomniano powyżej, obecność tej funkcji powoduje podatność sieci na różne formy ataku.

Jedną z możliwych form ataków jest metoda brute force, polegająca na próbie dopasowania każdej możliwej kombinacji 8 cyfrowego kodu PIN. Jest to niestety metoda niezwykle czasochłonna. Znalezienie odpowiedniego kodu potrwać może nawet kilka dni. W celu przyspieszenia procesu podjęto próbę użycia metody Pixie Dust, którą przeprowadzono za pomocą programu Reaver[29]. Program niestety nie mógł dopasować właściwego kodu, dlatego też podjęto kolejną próbę odgadnięcia kodu przy pomocy programu WiFi Warden[30]. Program ten próbuje wyliczyć kod PIN na podstawie informacji zebranych o sieci bezprzewodowej i urządzeniu mobilnym, na którym działa ta sieć. Wyliczenie kodu zakończyło się sukcesem po upływie zaledwie 3 minut, dzięki czemu możliwe było wydobycie hasła dostępowego do sieci wi-fi. Na rysunku 2 przedstawiono zrzut ekranu ze znalezionym hasłem do audytowanej sieci bezprzewodowej.

[29] Zob. stronę Internetową programu Reaver: <https://github.com/t6x/reaver-wps-fork-t6x>, 29 marca 2018 r.

[30] Program pobrać można ze sklepu Google Play.

Rysunek 2

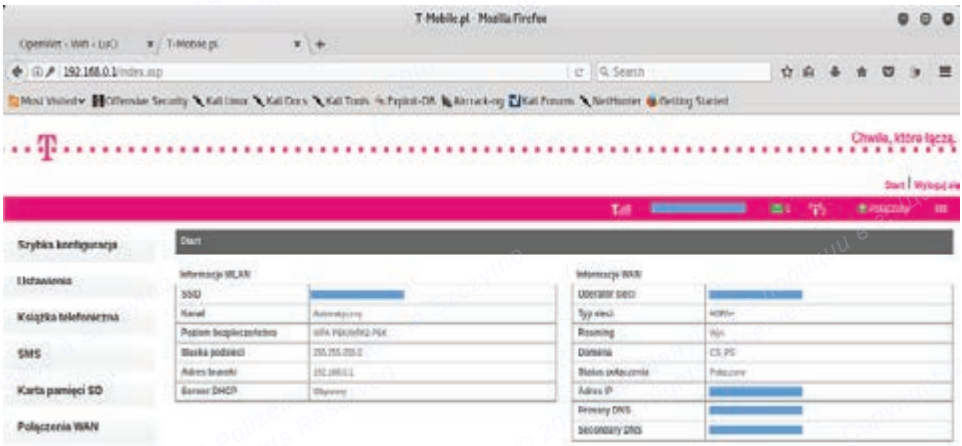
Znalezione hasło dostępowe do audytowanej sieci bezprzewodowej

Źródło: opracowanie własne — zrzut ekranu

Po udanym podłączeniu się do audytowanej sieci podjęto próbę zalogowania się na panel administracyjny routera. W tym celu użyto standardowej kombinacji producenta — login: admin, hasło: admin. Ponieważ użytkownik nie zmienił hasła do panelu administracyjnego routera logowanie zakończyło się pomyślnie i uzyskano dostęp do zaawansowanych ustawień urządzenia mobilnego. Rysunek 3 przedstawia panel administracyjny urządzenia mobilnego, które obsługuje audytowaną sieć wi-fi.

Rysunek 3

Panel administracyjny mobilnego routera wi-fi



Źródło: opracowanie własne — zrzut ekranu

Zważywszy na fakt, że urządzenie mobilne uzyskuje dostęp do Internetu poprzez sieć GSM, musi posiadać ono zainstalowaną kartę SIM, za pośrednictwem której możliwe jest nie tylko łączenie się z Internetem, ale również wykonywanie połączeń, czy też wysyłanie widomości SMS.

Uzyskując dostęp do panelu administracyjnego routera, możliwe staje się także odczytywanie i wysyłanie wiadomości bez wiedzy właściciela tego urządzenia. Może to w konsekwencji prowadzić do obciążenia jego rachunku kosztami za usługi, z których nigdy nie korzystał. Ponadto, uzyskując dostęp do czyjejś sieci, prawdopodobne jest, że wzrośnie wykorzystanie łącza, a co za tym idzie nastąpi spadek wydajności połączenia sieciowego. Co więcej osoba, która uzyskała nieautoryzowany dostęp do sieci, może dokonać naruszenia bezpieczeństwa komputerów i innych urządzeń będących w tej samej sieci. Możliwe jest także prowadzenie podsłuchiwania ruchu sieciowego oraz podszywanie się pod innych użytkowników sieci. Prowadzić to może między innymi do wykradzenia danych osobowych, danych niezbędnych do prowadzenia transakcji bankowych, a także zainfekowania urządzeń złośliwym kodem. Dodatkowo nie jest wykluczone, że zarażone urządzenia mogą stać się częścią botnetu, stworzonego w celu prowadzenia ataków hakerskich lub wydobywania walut kryptograficznych.

Jak wynika z przeprowadzonych badań, stosowanie standardowych zabezpieczeń ustawionych w sposób domyślny przez producentów sprzętu jawi się jako niezbyt dobry pomysł zważywszy na fakt, że ustawienia te mogą narazić nieświadomego użytkowania na niebezpieczeństwo kompromitacji zabezpieczeń sieciowych. Dlatego tak ważnym działaniem jest, aby zmienianie standardowych ustawień zabezpieczeń urządzeń mobilnych. Efekty braku działania użytkownika jest zwiększanie ryzyka przełamania zabezpieczeń, a tym samym narażenia się na możliwość

wykradzenia danych osobowych oraz innych danych, które postrzega się za wartościowe.

Prognozy zagrożeń

W 2004 r. odnotowano pierwszego wirusa na telefonie komórkowym. Obecnie codziennie w Polsce 280 tys. urządzeń jest infekowanych wirusami[31]. Eksperci od bezpieczeństwa są zgodni, że liczba zagrożeń dotyczących urządzeń mobilnych będzie rosła. Głównym celem będzie system Android, natomiast cyberprzestępcy nadal będą próbowali wykorzystywać sklep Google Play do dystrybucji szkodliwego kodu. Będą to głównie trojany bankowe i ransomware.

Wraz z rozwojem technologii i rozwojem urządzeń mobilnych możliwe jest korzystanie z zasobów wiedzy opartych na chmurze również poprzez smartfony, jednocześnie daje to możliwość włamanie się do telefonu poprzez bardziej innowacyjne metody. Doskonaleniu technologii towarzyszy rozwój technologii wykorzystywanych do przestępstw.

Obecnie w bankowości mobilnej istnieje zdecydowanie większe ryzyko nieuprawnionego dostępu do konta w bankowości internetowej. Urządzania mobilne narażone są na ataki hackerskie, istnieje bowiem niebezpieczeństwo przesłania czy to SMS-em, czy e-mailem wirusa lub programu szpiegowskiego. Najsłabszym ogniwem jest jednak stacja przekazująca sygnały telefonów komórkowych, ponieważ transmitowane dane mogą być przejęte przez hakerów.

Problemem jest także kradzież telefonu komórkowego. Można oczywiście zadzwonić do banku i zablokować swój rachunek, jednak złodziej ma przewagę w postaci czasu. Historia bankowości mobilnej jest krótka, ale innowacyjna i dynamicznie rozwojowa. Obok obecnie wykorzystywanych systemów Business Intelligence, które umożliwiają szczegółową analizę danych o aktywności klientów, opierając się na rozwiązania Big Data, może pojawić się technologia kryptograficzna Blockchain. Nowy trend może odegrać już niedługo kluczową rolę w transformacji sektora bankowego i bezpieczeństwa płatności. Jednak głównym elementem — najmniej pewnym — pozostaje człowiek.

Co zrobić, by być bezpiecznym?

Najwięcej bezpieczeństwa może zapewnić sobie sam człowiek. W bardzo zmiennym środowisku techniki i technologii, w którym nie wszyscy jego użytkownicy działają dla wspólnego dobra, konieczne jest przestrzeganie zidentyfikowanych zasad, których stosowanie podnosi poziom bezpieczeństwa, nie daje on jednak stuprocentowej gwarancji (tabela 2).

[31] PwC, *Technologie...*, wyd. cyt.

Tabela 2

Zasady bezpieczeństwa urządzeń mobilnych

Zasada	Opis
Hasła	W każdej aplikacji powinno być inne i oryginalne. Do zarządzania wieloma hasłami pomagają specjalne aplikacje, np. KeePass Password Safe 2,38 (spolszczone)
Oprogramowanie zabezpieczające	Zainstalowanie oprogramowania, które zablokuje pobieranie ryzykowanych aplikacji czy plików, skanuje pliki w poszukiwaniu złośliwego oprogramowania, blokuje spam, złośliwe treści, pozwala zlokalizować zagubiony telefon
Tylko zaufane hotspoty Wi-Fi	Należy korzystać z aplikacji mobilnych, gdy jesteśmy połączeni z zaufaną siecią Wi-Fi, np. domowa, w pracy. W smartfonach należy odznaczyć pole „automatyczne połącznia w przyszłości", co pozwoli na ograniczenie połączeń z sieciami publicznymi i ochronę danych prywatnych
Recenzje aplikacji	Przeglądanie informacji o bezpieczeństwie danej aplikacji
Ograniczony dostęp	Jeśli brak recenzji o bezpieczeństwie interesującej nas aplikacji, to należy sprawdzić, do jakich informacji na smartfonie czy tablecie aplikacja, którą chcemy zainstalować, żąda dostępu. Lepiej unikać udzielenia pozwolenia do książki telefonicznej z kontaktami, kont skonfigurowanych na urządzeniu, ID abonenta, czy dokładnej lokalizacji
Zaufane źródła aplikacji	Należy pobierać aplikacje wyłącznie z zaufanych i sprawdzonych źródeł, takich jak App Store czy Google Play
Wieloskładnikowe uwierzytelnianie	Oznacza kilkustopniową weryfikację tożsamości. Do takiej weryfikacji można wykorzystać np. hasło i smartfon (coś, co użytkownik zna, i coś, co posiada). Taka kombinacja jest jedną z najskuteczniejszych metod obrony przez nieautoryzowanym dostępem do konta użytkownika. Narzędzia takie jak np. True Key™ od Intel Security umożliwiają logowanie do kont i aplikacji z wykorzystaniem kilku składników, unikalnych dla danego użytkownika (np. rozpoznawania twarzy i urządzenia, które posiada) pozwala także zlokalizować zagubiony telefon

Źródło: opracowanie na podstawie artykułu: K. Mocek, *Jak dbać o bezpieczeństwo urządzeń mobilnych?*, <https://www.pcformat.pl/News-Jak-dbac-o-bezpieczenstwo-urzadzen-mobilnych,n,13666?utm_source=paste&utm_medium=paste&utm_campaign=chrome>, 13 grudnia 2018 r.

Wśród zaleceń dla firm, banków instytucji finansowych, w których korzysta się z urządzeń mobilnych, pojawia się konieczność wdrożenia zarządzania ryzykiem, które powinno być podstawą budowy systemu

bezpieczeństwa firm i organizacji. W standardach, takich jak np. norma ISO/IEC 27002, w rozdziale 6.2.1. *Polityka stosowania urządzeń mobilnych*, zaleca się organizowanie szkoleń dla pracowników korzystających z urządzeń mobilnych w celu podniesienia ich świadomości w zakresie zwiększonego ryzyka wynikającego z tego sposobu pracy i zabezpieczeń zalecanych do wdrożenia. W przypadku indywidualnych użytkowników zalecenia są podobne jak w przypadku pracowników, dla których zachowanie bezpieczeństwa powinno się rozpoczynać od oddzielenia prywatnego i służbowego wykorzystania urządzeń. W rozdziale 9.3 odpowiedzialność użytkowników prezentowane są zachowania, które mogą wypłynąć na poprawę bezpieczeństwa informacji poufnych, jeśli będą stosowane. W odniesieniu do urządzeń przenośnych zalecane są działania w postaci unikania zapisu informacji poufnych na tych urządzeniach, oczywiście jeśli jest to możliwe.

Innowacyjnym podejściem do zwalczania zaawansowanych zagrożeń jest wykorzystanie założeń blockchain[32] do poprawy bezpieczeństwa. Technologia blockchain umożliwia przechowywanie danych w rozproszony, zdecentralizowany sposób. To zapobiega wyciekom dużych ilości danych i umożliwia przeciwdziałanie manipulowaniu danymi, ponieważ wszelkie zmiany są od razu widoczne dla wszystkich podłączonych do danej sieci blockchain[33].

Google i Apple w sposób ciągły poprawiają bezpieczeństwo, aby zapobiegać instalacji szkodliwego oprogramowania, wdrażając między innymi uczenie maszynowe — co powinno zapobiegać pobieraniu przez użytkowników podejrzanych aplikacji.

Zakończenie

Przybywa zarówno urządzeń mobilnych, jak i e-usług. Klienci „bankują" na smartfonach, płacą telefonami, zaczynają rozmawiać z robotami. Transakcje online to wyzwanie czasu rzeczywistego, tym bardziej wobec zwiększającej się liczby dynamicznie ewoluujących zagrożeń. Niedawno zostały zidentyfikowane równocześnie dwie luki Meltdown, Spectre w architekturze większości procesorów, których używa się na świecie, włączając w to wyspecjalizowane procesory do obsługi systemów chmurowych. Koniecznością staje się coraz większe zaangażowanie w przeciwdziałanie atakom, włączając w działania metody numeryczne i AI, wyszukiwanie anomalii, predykcję rozpoznawanie zachowań i odchyleń.

[32] Blockchain jest to baza danych składająca się z informacji rozproszonych w Internecie zabezpieczona kryptograficznie. Poziom zabezpieczenia danych bloków jest wysoki, tak że nie istnieje możliwość zamiany zapisanych informacji, a jednocześnie są one łatwe do zweryfikowania — zob. H. Świeboda, *Ekonomiczne aspekty kryptowalut*, „Ekonomiczne problemy usług" 2018, nr 2(131), s. 371–378.

[33] T. Kowalczyk, *15 trendów bezpieczeństwa IT w 2018 r.*, „Computerworld" 2018, nr 1, s. 55.

Słowa kluczowe: urządzenia mobilne, zagrożenia, bezpieczeństwo

Streszczenie: Artykuł poświęcony jest problemowi identyfikacji zagrożeń oraz zasadom bezpieczeństwa urządzeń mobilnych. Ilość usług w cyberprzestrzeni stale się zwiększa i coraz chętniej wykorzystywane są do prowadzenia tego typu działalności urządzenia mobilne. Bardzo często na urządzeniach mobilnych przechowuje się nie tylko dane prywatne, ale również służbowe. Wyciek poufnych informacji z firmy czy przedsiębiorstwa jest bardzo niebezpiecznym zjawiskiem, ale użytkownicy często nie zdają sobie sprawy z zagrożeń. Niektórych zagrożeń udałoby się uniknąć, gdyby użytkownicy przestrzegali zasad bezpieczeństwa urządzeń mobilnych.

Keywords: mobile devices, threats, security

Summary: The number of services in cyberspace is constantly growing and mobile devices are more and more willingly used. Very often, not only private but also business data are stored on mobile devices. The leak of confidential information from a company or company is a very dangerous phenomenon, but users often do not realize the risks. Some threats would be avoided if users adhered to the security rules of mobile devices.

The article were devoted to the problem of hazard identification and security principles of mobile devices.