Nierówności Społeczne a Wzrost Gospodarczy, nr 53 (1/2018)
DOI: 10.15584/nsawg.2018.1.15 **ISSN 1898-5084**

dr Grzegorz Podgórski[1]
Katedra Informatyki, Wydział Zarządzania
Uniwersytet Łódzki

Bezpieczeństwo informacji w modelu BYOD

Wprowadzenie

Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji w dzisiejszym świecie opartym na technologiach teleinformatycznych jest kluczowym zagadnieniem. Rosnący udział w rynku urządzeń mobilnych, a także technologie, które wspomagają ten rozwój powodują, że w ostatnich latach można zaobserwować coraz dynamiczniej rozwijający się trend polegający na większym udziale urządzeń mobilnych w strukturach IT organizacji niż w latach ubiegłych. Wzrost ten można tłumaczyć coraz szerszą gamą urządzeń, jakie są obecnie oferowane na rynku, a co za tym idzie – rosnącym udziałem sprzedaży tychże urządzeń. Popularność tych urządzeń związana jest także z rozwojem technologii wspierających ich wykorzystanie nie tylko do zabawy czy też komunikacji, ale także do pracy. Coraz szybsze sieci telekomunikacyjne i bezprzewodowe, technologie takie jak Cloud Computing czy też dostępność aplikacji sprawiają, że trend ten z roku na rok jest coraz większy. Dla pracodawcy, jak i pracownika istotnym elementem jest możliwość wykorzystania tychże urządzeń do codziennej pracy zawodowej. Dla pracownika jest to dodatkowa możliwość, gdzie słowo „być w pracy" nabiera zupełnie nowego znaczenia. Dla pracodawcy danie takiej możliwości wymaga kompleksowego i przemyślanego podejścia, które pozwoli utrzymać odpowiedni poziom bezpieczeństwa informacji oraz dostępności usług informatycznych. Zabezpieczenie informacji i utrzymanie odpowiedniego poziomu bezpieczeństwa w przypadku tradycyjnego modelu pracy nie jest zadaniem łatwym. Natomiast w przypadku modeli pracy takich jak Bring Your Own Device staje się jeszcze większym wyzwaniem. Związane są z nim nie tylko aspekty finansowe na same zabezpieczenia, ale także przemyślania strategia związana z poziomem wsparcia technicznego

[1] Adres korespondencyjny: Uniwersytet Łódzki, Katedra Informatyki, ul. J. Matejki 22/26, 90-237 Łódź; e-mail: gpodgorski@wzmail.uni.lodz.pl; tel. 42 635 50 45.

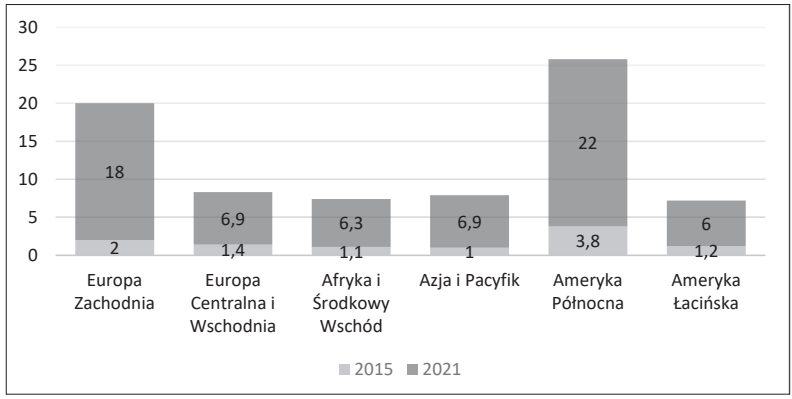
dla użytkowników, zakupem odpowiednich narzędzi, rozpatrzeniem kwestii prawnych, a także licencyjnych. Celem artykułu jest przedstawienie problemu bezpieczeństwa informacji w przypadku korzystania z modelu BYOD w organizacji oraz wskazanie kluczowych aspektów bezpieczeństwa związanych z tym modelem ze szczególnym uwzględnieniem elementów PBI (Polityki Bezpieczeństwa Informacji) i narzędzi informatycznych.

Model byod

Z modelu BYOD korzystają głównie młodzi ludzie w przedziale wiekowym 20–29 lat, uważanego za pokolenie „Generacji Y". Jest to pokolenie, które aktywnie wykorzystując nowinki technologiczne korzysta z mediów i technologii cyfrowych. Pokolenie to cechuje również podejście do pracy zgoła inne niż to, które reprezentowały poprzednie pokolenia. Dużą wagę przywiązują do życia prywatnego, oczekując od pracodawcy dużej swobody i elastycznego czasu pracy. Mając duży apetyt na życie nie chcą go w żaden sposób ograniczać, a już na pewno nie przez pracę. Uważani są za nielojalnych pracowników, którzy nie przywiązują się do firmy i stanowiska i bardzo chętnie się z nią rozstaną, jeśli tylko znajdzie się lepsza okazja lub dana firma za bardzo będzie ingerować w ich życie i swobody. Według różnych badań przeprowadzanych na całym świecie trend BYOD staje się coraz bardziej popularny wśród organizacji, nie tylko tych działających w sferze IT. Zwolennicy tego modelu pracy uważają go za naturalny etap rozwoju przedsiębiorstwa.

Potencjał tego modelu nierozerwalnie związany jest w dużej mierze z technologią chmury obliczeniowej (*Cloud Computing*). Obecnie ponad 31% organizacji w Polsce korzysta z usług chmury obliczeniowej. Według szacunków wartość rynku związanego z usługami w chmurze w 2019 roku przekroczy 450 mln dolarów. Na uwagę zasługuje również fakt, iż migracja organizacji do usług w chmurze nie jest związana z branżą, w jakiej działają te organizacje oraz ich wielkością.

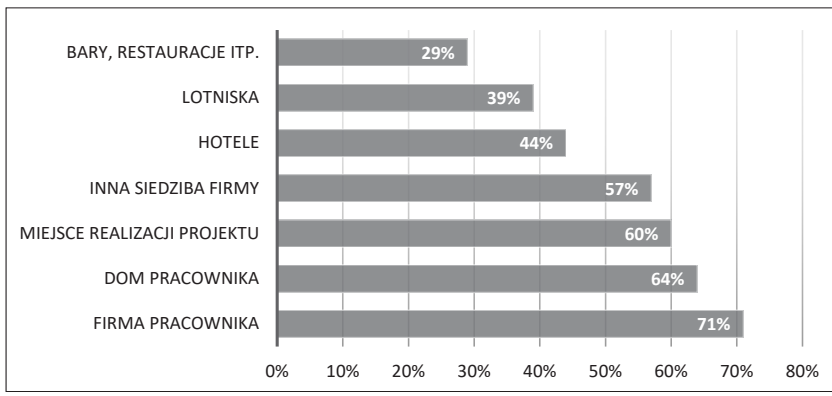
Na świecie można obecnie zaobserwować rosnącą tendencję związaną z pracą mobilną oraz mobilnością samych użytkowników. Wielcy giganci na rynkach technologicznych tacy jak Citrix czy też Cisco przewidują, że prawdziwą przyszłością w kierunku, której organizacje będą podążać jest mobilny styl pracy oraz wzrost znaczenia mobilności. Tylko w Polsce, jak wynika z badań przeprowadzonych w 2015 roku, jest ponad 19 milionów smartfonów [Mikowska, (http)]. Firma Citrix przewiduje, iż do 2020 roku 89% organizacji będzie oferować mobilny styl pracy [Citrix, (http)]. Już dziś ilości danych, jakie rocznie są przesyłane przez sieci komórkowe jest gigantyczna, a prognoza na lata 2016–2021 wynosi 1600 ExaBytów [Ericsson, (http)]. Miesięczne wartości przysyłu danych dla poszczególnych regionów świata ilustruje rys. 1.



Rys. 1. Ilość miesięcznych danych przesyłanych w GB z użyciem smartfonów dla wybranych regionów świata z prognozą na lata następne

Źródło: opracowanie własne na podstawie: [Ericsson (http)].

Firma Citrix w swoich prognozach na rok 2020 dotyczących mobilnego trybu pracy przewiduje zmiejszenie przestrzeni pracowniczej o 18% [Citrix, (http)]. W obecnej chwili większość dużych organizacji w związku ze wzrostem mobilnego stylu pracy oferuje 7 biurek na każdych 10 pracowników i tendencja ta, jak pokazują raporty, jest malejąca. Ogólnoświatowe badania wykazują także, że pracownicy coraz częściej korzystają także z miejsc do pracy zlokalizowanych poza biurem wykonując swoje czynności zawodowe – rys. 2.



Rys. 2. Miejsca aktywności zawodowej pracowników

Źródło: opracowanie własne na podstawie [Citrix, (http)].

Jak widać, czy tego chcemy czy też nie tendencje światowe oraz prognozy na lata przyszłe pokazują nieunikniony wzrost znaczenia pracy mobilnej, dostępności usług oraz ogólnie pojętej mobilności użytkowników. Badania firmy Cisco

przeprowadzone w latach 2013–2016 wskazują na wzrost liczby urządzeń BYOD o 105% z 198 do 405 mln [Loucks, (http)]. Model BYOD jest najczęściej wybieranym modelem przez organizacje. Jest to też najbardziej dynamicznie rozwijający się obecnie trend w organizacjach.

ASPEKTY BYOD ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

Jak już wspomniano wcześniej, model BYOD rozwija się bardzo dynamicznie, nie tylko w organizacjach zajmujących się głównie IT, ale dotyka wszelkie organizacje zarówno te prywatne, jak i państwowe w różnych sektorach. Model ten przynosi ze sobą wymierne korzyści dla pracodawcy, jak i samych pracowników. Niestety, budzi on także duży niepokój zwłaszcza, jeśli chodzi o ochronę danych, dostęp do infrastruktury IT organizacji, a także obsługę nowych urządzeń spoczywającej na barkach działów IT. Obawy związane z bezpieczeństwem danych w modelu BYOD nie są bezpodstawne. Nawet w przypadku standardowego modelu pracy na urządzeniach w pełni kontrolowanych przez organizację stopień ryzyka wycieku czy utraty danych jest wysoki, a co dopiero w przypadku prywatnych urządzeń, nad którymi dział IT może nie mieć całkowitej kontroli. Z badań przeprowadzonych w kwietniu 2013 roku przez firmę Check Point Software wynika, iż największym zagrożeniem stają się urządzenia mobilne [Check Point, (http)].

Zastosowanie BYOD w organizacji jest powodem różnych problemów i kwestii formalnych, które muszą być rozwiązane. Głównym problemem jest oczywiście problem zapewnienia bezpieczeństwa. Drugim nie mniej istotnym jest zapewnienie przez organizację odpowiedniej pomocy technicznej ze strony działu IT dla pracowników i ich urządzeń. W przypadku standardowego modelu pracy to dział IT miał decydujący wpływ na decyzję, co do kupowanego sprzętu, systemów operacyjnych i aplikacji na nim się znajdujących. W przypadku modelu BYOD dział IT staje przed nowym wyzwaniem, jakim jest wsparcie dla wielu systemów operacyjnych, szeregu aplikacji jak również wspierania różnorakich modeli i typów urządzeń. Tylko 22% firm zgadza się na korzystanie ze wszystkich urządzeń, które posiada pracownik. Większość, bo 71% organizacji wprowadzających BYOD zapewnia wsparcie tylko dla wybranych urządzeń posiadanych przez pracowników. Nie bez znaczenia jest sam system operacyjny, który obsługuje mobilne urządzenie. Dla przykładu dwie z najbardziej restrykcyjnych organizacji, jeśli chodzi o bezpieczeństwo Agencja Bezpieczeństwa Narodowego USA (NSA – *National Security Agency*) oraz Departament Obrony (DoD – *Department of Defense*) zgodnie stwierdzili, że poza urządzeniami BlackBerry nie mają żadnego wyboru w kwestii wyposażania pracowników swoich agencji w smartfony. Według [BYOD&Mobile, (http)] w kwestii wsparcia systemów operacyjnych w modelu BYOD system iOS uzyskał 76% w 2014 r. i 72% w 2013 r.

Następnie uplasowały się takie systemy jak Android 69% i 61% (odpowiednio dla roku 2014 i 2013), Windows 66% i 51% (rok 2014 i 2013) oraz RIM (Blackberry) 40% i 48% (odpowiednio w roku 2014 i 2013). To ukazuje skalę problemu, z jakim każda organizacja musi się zmierzyć planując wdrożenie BYOD w swojej organizacji. Szereg urządzeń, systemów operacyjnych i aplikacji, które mogą być potencjalną luką w szczelnym systemie ochrony danych w organizacji. Wsparcie dla wielu systemów operacyjnych przekłada się na zwiększone koszty związane z utrzymaniem, wyszkoleniem i wyposażeniem działów IT w organizacji. Wpływa to także nie tylko na koszty, ale także na czas, jaki poświęcają działy helpdesk na rozwiązywanie problemów użytkowników – co deklaruje aż 14% respondentów, wskazując to jako negatywny skutek wdrożenia bezpieczeństwa dla urządzeń mobilnych. Wdrożenie BYOD w organizacji to wyzwanie wymierzone szczególnie w dział IT, który poniesie największe koszty z tym związane – zarówno te finansowe, które pozwolą utrzymać odpowiedni poziom bezpieczeństwa, jak i te związane z pracą własną, szkoleniami i zakupem oprogramowania. Nietrudno wyobrazić sobie sytuację pracownika przychodzącego do pracy z tabletem z system operacyjnym bez aktualizacji, który musi posiadać dostęp do informacji poufnych. Na uwagę zasługuje również fakt, iż jedynie 14% kosztów związanych z BYOD ma związek ze sprzętem, co podkreśla wagę wyboru właściwych modeli nadzoru i pomocy technicznej, aby móc zachować kontrolę nad kosztami. Organizacje, które wdrożyły rozwiązania typu BYOD w większości, bo aż 58% zapowiadają wzrost wydatków związanych z IT, a aż 37% nie jest pewnych co do przyszłych kosztów.

Istnieje wiele zagrożeń wynikających zarówno z wykorzystania samych urządzeń mobilnych w organizacji jak również związanych z tym, iż są to urządzenia prywatne. Wraz z głównymi zagrożeniami wynikającymi z modelu BYOD umieszczono wartości procentowe jakie odnotowano w odpowiedziach respondentów [BYOD&Mobile, (http)]:
– utrata danych – 72%,
– nieautoryzowany dostęp do danych lub systemów – 56%;
– nieautoryzowany dostęp do infrastruktury IT organizacji – 56%,
– kradzież urządzenia mobilnego – 50%,
– ryzyko infekcji szkodliwym oprogramowaniem – 54%,
– wyciek firmowych danych – 72%,
– brak pełnej kontroli nad prywatnymi urządzeniami – 48%,
– niezabezpieczone systemy operacyjne – 39%,
– brak dostatecznych metod zabezpieczenia mobilnego urządzenia – 37%,
– niezaakceptowane aplikacje na urządzeniach prywatnych,
– brak lub niedostateczna ochrona antywirusowa i antyphishingowa;
– problemy z kwestiami prawnymi – 38%

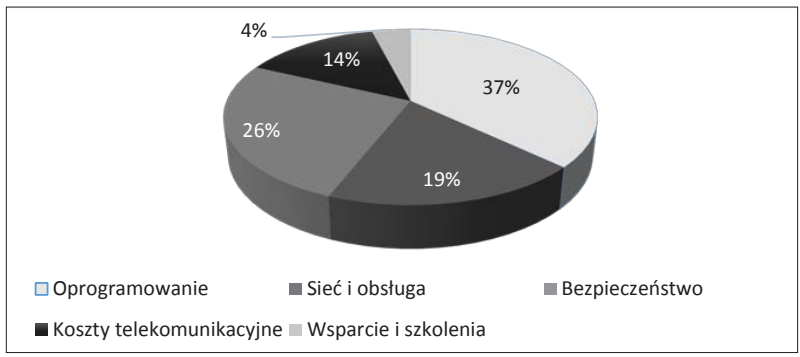
Firmy czy też organizacje wdrażające modele BYOD powinny poświęcić szczególną uwagę jeszcze dwóm aspektom bardzo często pomijanym, a miano-

wicie aspektom prawnym jak i licencyjnym. Niestety, nie tylko w tym przypadku polskie ustawodawstwo nie do końca nadąża nad zmianami w realnym świecie i trzeba się liczyć z dużą niedoskonałością także w tym aspekcie. Trudno szukać jakiś regulacji związanych z modelem BYOD w polskim systemie ustawodawczym. Jedyna wzmianka związana z pracą wykonywaną przy pomocy własnych urządzeń jest zawarta w kodeksie pracy w art. 67 § 2 i odnosi się do telepracy. Natomiast w art. 94 tegoż kodeksu wyraźnie można przeczytać, iż to pracodawca ma obowiązek dostarczyć narzędzi pracy pracownikowi. W związku z tym nie można pracownikowi narzucić obowiązku pracy na własnym urządzeniu – może to być jedynie forma obustronnego porozumienia między pracodawcą a pracownikiem. Bardzo ważne jest, aby pracownik miał zawsze alternatywę wybierając taki model pracy bez wymuszania na nim takiej decyzji. Jest to szczególnie istotne, ponieważ można było zauważyć już takie wyroki sądów administracyjnych, które kwestionowały takie porozumienia, jako wymuszenia na pracownikach [wyrok NSA z dnia 01.12.2009 r., I OSK 249/09]. Należy także pamiętać, iż prywatne urządzenie, które zostaje objęte firmowym system bezpieczeństwa i nadzoru powoduje, że system taki w mniejszym lub większym stopniu ingeruje w samo urządzenie i dane w nich przechowywane. Ze względu na brak uregulowań prawnych co do takiej ingerencji w prywatne urządzenie przez pracodawcę koniecznością jest sporządzenie odpowiednich uregulowań na poziomie pracodawcy i pracownika, czyli na poziomie danej organizacji. Już samo monitorowanie przez pracodawcę urządzenia należącego do pracownika bez jego zgody może narazić pracodawcę na sankcje prawne. Jest to szczególnie istotne w przypadku wszelkich urządzeń, na których oprócz danych firmowych mogą i znajdują się dane prywatne, w skład których mogą także wchodzić dane osobowe – zarówno te należące do pracownika, jak i pracodawcy. Dlatego tak ważna jest pisemna obustronna klauzula obejmująca czynności wykonywane po stronie pracownika i pracodawcy. W klauzuli takiej powinny znaleźć się takie prawa pracodawcy, jak możliwość:
– stosowania zabezpieczeń informatycznych na urządzeniu pracownika;
– form oraz zakresu monitorowania urządzenia;
– usuwania w razie konieczności danych firmowych z urządzeń pracownika.

W związku z tym stosowny aneks do umowy czy też inne pisemne porozumienie w tej sprawie powinno jawnie i w sposób szczegółowy określać czynności, jakie może wykonywać pracodawca w stosunku do prywatnej własności pracownika, który wykorzystuje takie urządzenie do pracy. Po stronie pracownika klauzula taka także powinna dawać mu poczucie bezpieczeństwa oraz prywatności i poufności prywatnych danych przechowywanych na takim urządzeniu. Jest to szczególnie trudne ze względu na to, iż w wielu przypadkach bardzo ciężko rozdzielić miejsce przechowywanie danych firmowych od danych prywatnych.

Wysokie przychody osiągane dzięki wprowadzeniu modelu BYOD dają organizacjom ogromne możliwości. Nie należy jednak zapominać o ścisłej kontroli wydatków przeznaczanych na tego typu rozwiązanie. Wyniki badań wskazują

jednoznacznie, że w przypadku pełnego wdrożenia BYOD 37% wszystkich wydatków związanych jest z oprogramowaniem (potrzebnym do zarządzania, monitorowania, jak również zapewnienia bezpieczeństwa), a kolejne 26% na samo bezpieczeństwo (rys. 3). Jak wykazują badania, tylko w przypadku strategicznego, pełnego wdrożenia BYOD korzyści przewyższają koszty. Dlatego tak ważne jest świadome zaplanowanie i kompleksowe podejście do problemu. Zagwarantowanie właściwej obsługi rozwiązania BYOD w organizacji będzie korzystne zarówno dla organizacji, jak i dla pracowników.



Rys. 3. Rozkład kosztów związanych z wdrożeniem modelu BYOD

Źródło: opracowanie własne na podstawie [Loucks, (http)].

BEZPIECZEŃSTWO INFORMACJI W MODELU BYOD

Utrzymanie odpowiedniego poziomu bezpieczeństwa w przypadku mobilnych użytkowników nie jest zadaniem łatwym, a w przypadku mobilnych użytkowników pracujących w modelu BYOD jest jeszcze trudniej. Wiąże się to głównie z niemożnością otrzymania pełnej kontroli nad mobilnym urządzeniem, gdyż mówimy tutaj o urządzeniu prywatnym. Te organizacje, które już wprowadziły mechanizmy ochrony dla użytkowników mobilnych mają ułatwiony start do zapewnienia bezpieczeństwa w modelu BYOD. Istnieje wiele różnic pomiędzy urządzeniami stacjonarnymi, które są w pełni własnością organizacji a tymi, które są urządzeniami prywatnymi wykorzystywanymi do pracy w modelu BYOD. Główne różnice to:

– brak dostępu na poziomie administracyjnym lub na poziomie root;
– bardzo skomplikowany proces aktualizacji samego systemu operacyjnego, jak również aplikacji na nim się znajdujących;
– wiele ograniczeń, które narzuca sam system operacyjny;
– ciągła obecność w sieci, jak również podłączanie do sieci niezabezpieczonych i niezaufanych;
– szeroki wachlarz zagrożeń: kradzież urządzenia, ataki na aplikację, fałszywe aplikacje, fałszywe sieci bezprzewodowe itp.;

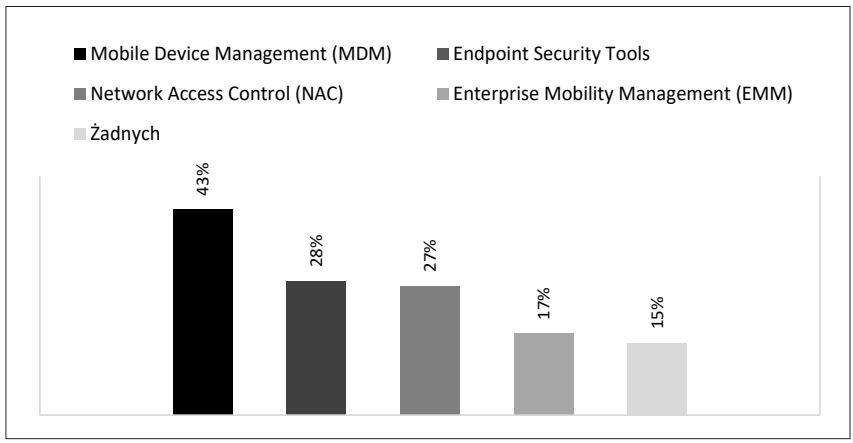
– niska możliwość kontroli zainstalowanych aplikacji;
– wysokie uprawnienia użytkowników.

Różnice te sprawiają, że wdrożenie i utrzymanie odpowiedniego poziomu bezpieczeństwa zwłaszcza dla organizacji, która nie miała do tej pory do czynienia z pracownikami mobilnymi jest szczególnie trudne i wymaga wielu przemyślanych decyzji oraz dużej wiedzy. Wdrażanie takiej ochrony powinno być dobrze zaplanowane i stosownie wdrożone i co najważniejsze powinno być kompleksowe.

Kluczowe zagadnienia związane z kwestiami bezpieczeństwa dla organizacji wynikające z modelu BYOD wymienione zostały poniżej:
– identyfikacja urządzeń (*FingerPrinting OS*);
– zarządzanie dostępem do danych;
– ochrona przed wyciekiem danych;
– ochrona danych, aplikacji i usług udostępnianych;
– zarządzanie bezpieczeństwem urządzeń mobilnych – prywatnych;
– dostępność usług;
– zaufanie do dostawcy i jego zabezpieczeń (*Cloud Computing*);
– zabezpieczenie transmisji;
– luki w oprogramowaniu aplikacji;
– luki w systemach operacyjnych;
– usunięcie danych po odejściu pracownika lub po kradzieży urządzenia;
– szkolenie i świadomość użytkowników.

Bardzo ważnym elementem takiego wdrożenia dotyczącego ochrony danych i informacji jest aktualizacja firmowej Polityki Bezpieczeństwa Informacji (PBI), szkolenia pracowników i członków działów IT oraz zakup odpowiedniej infrastruktury. Infrastruktura ta jest niezbędnym elementem, który gwarantuje sprawowanie kontroli nad mobilnym i prywatnym środowiskiem pracy, jaki pojawia się w organizacji. Pozwala ono na identyfikację urządzeń, monitorowanie ich zabezpieczeń, zarządzanie nimi, blokowanie dostępu z danych urządzeń, zdalną modyfikację ustawień dotyczących bezpieczeństwa, wycofywanie urządzenia z użycia, zarządzanie zasobami, zarządzanie aplikacjami oraz wdrażanie korporacyjnej polityki bezpieczeństwa. W związku z tym elementem składowym, bez którego nie ma mowy o BYOD są aplikacje typu MDM (z ang. *Mobile Device Management*). Oprogramowanie typu MDM umożliwia kompleksowe zarządzanie oraz monitorowanie mobilnych urządzeń, które mają dostęp do poufnych danych i usług. Coraz częściej aplikacje tego typu rozszerzane są o aplikację typu MAM (z. ang. *Mobile Application Management*) oraz MCM (z ang. *Mobile Content Management*) lub są częścią pakietu MDM. Zazwyczaj oprogramowanie takie składa się z wielu modułów odpowiadających za poszczególne funkcje takie jak: identyfikacja urządzenia, przydzielanie przywilejów, zdalne blokowanie skradzionych lub zgubionych urządzeń, aktualizujące a także alarmujące użytkownika o niebezpieczeństwie lub niedozwolonej aktywności [Madden, 2014, s. 17]. Zasady działa-

nia tego typu oprogramowania są w zależności od producenta oprogramowania trochę różne natomiast końcowy efekt jest taki sam – poprawa bezpieczeństwa i kontrola nad urządzeniami mobilnymi. Oczywiście, to czy wszystkie moduły tego typu oprogramowania – łącznie z agentowymi instalowanymi na prywatnych urządzeniach – zostaną zaimplementowane, zależy tylko wyłącznie od firmy. Typy narzędzi, jakie organizacje wykorzystują przedstawia rys. 4.



Rys. 4. Typy narzędzie wykorzystywane w modelu BYOD

Źródło: opracowanie własne na podstawie [BYOD&Mobile, (http)]

Jaki jest więc najważniejszy element układanki, jakim jest zapewnienie bezpiecznego środowiska pracy dla modelu BYOD? Odpowiednio opracowana i wdrożona polityka BYOD wchodząca w skład PBI oraz infrastruktura typu MDM. Odpowiednie procedury, regulaminy i strategię działania wchodzące w skład PBI powinny określać takie elementy jak:

– jakiego typu urządzenia mogą pojawiać się w firmowej sieci – smartfon, tablet, laptop – oraz na jakich zasadach (czy potrzebna jest zgoda przełożonego? itp.);
– jakie systemy operacyjne oraz w jakiej wersji są dopuszczane i wspierane przez dział IT;
– jakie warunki musi spełniać używane urządzenie (np. możliwość szyfrowania danych, dostępność form łączności, zabezpieczenie dostępu do urządzenia);
– jakie oprogramowanie musi koniecznie na nim się znajdować – chodzi głównie o oprogramowanie antywirusowe, antyphishingowe, antyspyware'owe itp., jak również może to być dedykowane oprogramowanie agentowe;
– lista dozwolonych lub ewentualnie lista zakazanych aplikacji na prywatnych urządzeniach;
– procedury opisujące konfigurację, aktualizację oraz konserwację takich elementów urządzenia jak system operacyjny, system antywirusowy, zapora systemowa inne aplikacje i mechanizmy zabezpieczające;

– zabezpieczenia fizyczne bądź sprzętowe, które będą chronić dane w przypadku kradzieży urządzenia;
– procedura permanentnego kasowania danych z urządzenia w przypadku zwolnienia pracownika czy też sprzedaży przez niego urządzenia;
– określenie zasobów, do których będzie konfigurowany dostęp z tychże urządzeń;
– sankcje dyscyplinarne i karne w przypadku naruszenia procedur i/lub zaniedbań ze strony użytkownika.

Nie należy także zapominać, iż większość organizacji ma w swoich zasobach dane osobowe, które powinny podlegać trochę innym kryteriom ochrony. Wiąże się to także z innym podejściem do wprowadzanych zabezpieczeń w przypadku, kiedy użytkownicy w modelu BYOD mają mieć do takich danych dostęp. W takim przypadku należy ustalić:
– czy dane osobowe mogą być przetwarzane na urządzeniach mobilnych;
– gdzie dane osobowe mogą być przechowywane i przetwarzane;
– czy mogą, a jeśli tak to, w jaki sposób mogą być przenoszone lub przetwarzane na prywatnych urządzeniach oraz ewentualnie, jakie warunki muszą być ku temu spełnione;
– jakie jest ryzyko wycieku takich danych z urządzeń prywatnych;
– czy dane osobowe mogą się mieszać z prywatnymi danymi na urządzeniu pracownika;
– jakie powinny być mechanizmy zabezpieczające urządzenie mobilne, jeśli takie dane będzie przechowywać bądź przetwarzać;
– jaka procedura została wdrożona, by pracownik nie mógł przetwarzać danych, gdy nie będzie pracował w organizacji.

W raporcie [BYOD&Mobile, (http)] jako jedne z głównych w odniesieniu do modelu BYOD i bezpieczeństwa wyróżnia się:
– głównym aspektem jest utrzymanie mobilności użytkowników – 57%, ich satysfakcja – 56% i produktywność – 54%;
– główną bolączką instytucji jest utrata danych firmowych lub danych należących do klientów firmy – 67% oraz nieautoryzowany dostęp do danych i systemów w organizacji – 57%;
– wymaganie wprowadzenia dodatkowych nakładów IT na incydenty związane z bezpieczeństwem – 30%;
– jako jedno z głównych problemów z bezpieczeństwem wyróżnia się ryzyko ochrony haseł – 67%, zdalny dostęp do danych – 52% oraz użycie szyfrowania – 43%.

Jak widać, wdrożenie BYOD nie jest zadaniem łatwym ze względu na aspekty bezpieczeństwa. Jednak odpowiednio zaplanowane wdrożenie BYOD oraz dobrze opracowana Polityka Bezpieczeństwa Informacji pozwalają zapanować nad nowym wyzwaniem. Na pewno wymaga to stworzenia lub zmodyfikowania już istniejących strategii dotyczących infrastruktury IT, jak również i całej organizacji. Sporym wyzwaniem może być kontrola przepływu danych w urządzeniach mobilnych. Natomiast dzięki takim rozwiązaniom jak konteneryzacja zapewnia-

jąca oddzielenie danych firmowych od prywatnych, szyfrowanie czy też podnoszenie poziomu świadomości użytkowników poprzez szkolenia oraz infrastruktura MDM prawie każda organizacja może wdrożyć model pracy BYOD – choć na pewno nie będzie to proces łatwy ani tani. Jednak korzyści wynikające ze zwiększonej produktywności użytkowników, ich zadowolenia oraz korzyści finansowe powinny zrównoważyć lub nawet przewyższyć koszty.

ZAKOŃCZENIE

Bezpieczeństwo informacji w dzisiejszym świecie opartym na technologiach teleinformatycznych jest zagadnieniem kluczowym. Zagrożenia związane z bezpieczeństwem informacji towarzyszą nowym technologiom i rozwiązaniom od samego początku i nie inaczej jest także w przypadku modelu BYOD. Mając na uwadze wszelkie prognozy i statystyki dotyczące modelu BYOD oraz mobilności użytkowników można stwierdzić, iż wydaje się on być naturalnym etapem rozwoju obecnego świata, jak i każdej organizacji. Już dziś widzimy zmiany związane ze swobodnym dostępem do usług firmowych, ogólnodostępnymi sieciami bezprzewodowymi, chmurą obliczeniową, które powodują, że życie zawodowe łączy się i przeplata z życiem prywatnym. Coraz większa liczba organizacji decyduje się świadomie i kompleksowo na wdrożenie BYOD do swojej organizacji. Jeśli jest to działalność świadoma, to na pewno można liczyć na większy poziom bezpieczeństwa, jaki może taka organizacja zapewnić oraz na korzyści finansowe, jak i personalne. Nieświadoma zgoda na tego typu praktyki związane z prywatnymi urządzeniami w organizacji skazane są, niestety, na fiasko, zarówno pod względem bezpieczeństwa informacji, jak również na zalety finansowe związane z tego typu rozwiązaniem. Należy pamiętać, iż niemożliwe jest osiągnięcie 100-procentowego poziomu bezpieczeństwa. Można jednak, stosując odpowiednie procedury, strategie oraz mechanizmy zabezpieczeń zmniejszyć ryzyko wystąpienia zagrożeń, przez co zapewnić odpowiedni poziom bezpieczeństwa informacji. Model BYOD jest w tej kwestii swoistym wyzwaniem dla organizacji. Wraz z niemałymi korzyściami pojawiają się nowe niemałe wyzwania. Niestety, jak to często bywa za dynamicznie rozwijającymi się rozwiązaniami technologicznymi nie nadążają regulacje prawne.

BIBLIOGRAFIA

BYOD & Mobile Security 2016, www.gyartastrend.hu/download.php?id=27070 (dostęp: 01.09.2016 r.).

Check Point Check Point 2013 Security Report http://www.checkpoint.com/campaigns/security-report/ (dostęp: 01.09.2016 r.).

Citrix Workplace of the Future: a global market research report http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf (dostęp: 21.08.2016 r.).

Ericsson Mobility Report, http://www.ericsson.com/res/docs/2016/mobility-report/ericsson-mobility-report-feb-2016-interim.pdf (dostęp: 01.09.2016 r.).

Loucks J., Medcalf R., Buckalew L., Faria F., *Wpływ BYOD na finanse przedsiębiorstwa 10 najważniejszych ogólnych wniosków z badania programu Horizons grupy IBSG Cisco*, http://www.cisco.com/c/dam/en_us/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Top-10-Insights-PL.pdf (dostęp: 15.08.2016 r.).

Madden J., 2014, *Enterprise Mobility Management: Everything you need to know about MDM, MAM and BYOD, 2014 Edition,* Wyd. Jack Madden.

Mikowska M., *Polska jest Mobi*, http://www.tnsglobal.pl/coslychac/files/2015/05/POLSKA_JEST_MOBI_2015.pdf (dostęp: 01.09.2016 r.).

Streszczenie

Rozwój urządzeń mobilnych, który można zaobserwować obecnie, sprzyja ich wykorzystaniu nie tylko do komunikacji, czy rozrywki, ale także w coraz większym stopniu także do pracy. Nowe technologie takie jak Cloud Computing, szybkie oraz ogólnodostępne sieci bezprzewodowe, coraz doskonalsze urządzenia mobilne, których szeroki wachlarz dostępny na rynku powoduje, iż każdy użytkownik może dopasować je do swoich wymogów, a to sprawia, że coraz dynamiczniej rozwija się trend związany z mobilnością pracowników. Mobilność pracowników, a co za tym idzie – możliwość mobilnej pracy rozwija się bardzo dynamicznie i pozwala na wykorzystywanie coraz to nowszych rozwiązań technologicznych. Jednym z modeli, czy też trendów, które można zaobserwować jest BYOD (*Bring Your Own Device*). Jest to model, który pozawala na wykorzystanie swojego prywatnego urządzenia w celach służbowych. Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji w przypadku nowych technologii związanych z mobilnością użytkowników nie jest zadaniem łatwym. Dla organizacji oznacza to całkowitą zmianę podejścia do zarządzania siecią informatyczną, urządzeniami przenośnymi, zarządzania bezpieczeństwem oraz do zarządzania samymi użytkownikami. W artykule zaprezentowano główne aspekty związane z bezpieczeństwem informacji, które powinny się znaleźć w każdej organizacji, gdy ta wdraża lub wdrożyła model BYOD do swojej infrastruktury teleinformatycznej. Poruszone zostały także aspekty prawne, finansowe i związane z licencjonowaniem, które są bezpośrednio związane z modelem BYOD.

Słowa kluczowe: BYOD, mobilność użytkowników, bezpieczeństwo BYOD, bezpieczeństwo informacji

Information security in the BYOD model

Summary

The development of mobile devices, which can be seen now favors their use not only for communication, or entertainment, but increasingly also for work. New technologies such as Cloud Computing, fast, and public wireless networks, ever more perfect mobile devices, where a wide range available on the market makes that each user can adjust it to their requirements mean that more and more dynamically growing trend of workforce mobility. Mobility of workers, and thus the possibili-

ty of mobile computing is growing very rapidly and allows the use of newer and newer technologies. One of the models or trends that can be observed is BYOD (*Bring Your Own Device*). It is a model that allows for the use of their personal devices for business purposes. Ensure an appropriate level of information security in the case of new technologies related to user mobility is not an easy task. For organizations, this means a complete change of approach to managing the IT network, mobile devices, security management and management employees themselves. In the article will be presented the main aspects of information security, which should be in any organization which implements or has implemented a BYOD model for its IT infrastructure. Also it will be discussed the legal aspects, financial and related to licensing, which are directly connected with the BYOD model.

Keywords: BYOD, mobility of users, security of BYOD, information security

JEL: O33