Grzegorz Podgórski[1]

Mobilność użytkowników a bezpieczeństwo informacji w środowisku IT

1. Wstęp

Wraz z rozwojem urządzeń mobilnych oraz ich coraz szerszą dostępnością rozwinęły się także wszelkie usługi mobilne dla użytkowników. Obecnie nie wyobrażamy sobie braku dostępu do wielu aplikacji czy też usług z dowolnego miejsca, w którym się znajdujemy. Jednak mobilność użytkowników ma też swoją cenę. Jedną z nich, chyba najważniejszą dla organizacji, jest bezpieczeństwo. Jak zapewnić bezpieczeństwo danych, informacji i usług, kiedy muszą one być dostępne z dowolnego miejsca na Ziemi, w dowolnym urządzeniu i systemie operacyjnym? Jest to wyzwanie, które stoi przed wieloma organizacjami. Dla jednych jest już codziennością, w którą świadomie bądź też nie wkroczyły, podążając za trendem pracy mobilnej, dostępem mobilnym, czyli – ogólnie rzecz biorąc – za mobilnością swoich użytkowników. Dla innych – jak wskazują wszelkie prognozy i badania na świecie – krok nieunikniony, na który muszą się odpowiednio przygotować, tak aby okazał się dla nich opłacalny i jak najbardziej bezpieczny. W niniejszym artykule zostaną zaprezentowane główne kwestie związane z mobilnością użytkowników w kontekście bezpieczeństwa informacji, ze szczególnym uwzględnieniem aspektów prawnych oraz finansowych. Najważniejsze wnioski dotyczące zagadnień bezpieczeństwa danych zostały opracowane na podstawie doświadczeń własnych autora oraz studiów literaturowych.

2. Mobilność użytkowników w środowisku IT

Pisząc o mobilności, warto na początku określić, co przez nią będziemy rozumieć. Czy chodzi tylko o mobilność pracy, czy dostęp mobilny, czy też

[1] Uniwersytet Łódzki, Wydział Zarządzania.

elastyczność w dostępie do pewnych usług i danych? Otóż definiując mobilność, warto wskazać kilka aspektów jej funkcjonowania. Zgodnie ze *Słownikiem języka polskiego PWN* mobilny to taki, który łatwo daje się wprawić w ruch. Jeśli przenosimy więc to wyrażenia do środowiska IT, potrzebne są nam jakieś mechanizmy (rozwiązania), które w prosty sposób umożliwiają użytkownikom dostęp do usług i zasobów IT, nieograniczony jedynie do miejsca ich pracy stacjonarnej. Ponadto – jak czytamy w dalszej części definicji słowa – mobilny to zdolny do sprawnego, elastycznego działania. Także w tym wypadku nie chodzi tylko o uzyskanie przez użytkownika dostępu do pewnych danych i usług, ale o możliwość ich elastycznego wykorzystania, co można by tłumaczyć jako dostęp z dowolnego miejsca, dowolnego urządzenia z dowolnym systemem operacyjnym, nie wspominając o elastyczności działania, jaką powinien mieć sam użytkownik. Samą istotę mobilności użytkowników oddaje trzecia część definicji, która określa, że mobilny oznacza „często zmieniający miejsce pobytu lub miejsce pracy". Jak widzimy, słowo „mobilny" pozwala na dosyć szeroką interpretację w zależności od aspektu, w jakim będziemy chcieli je rozważać. W niniejszym artykule ilekroć będę wspominał o mobilności użytkowników, za każdym razem będę miał na myśli te trzy aspekty słowa „mobilny", czyli łatwość przemieszczania, elastyczność działania (dostępność w ruchu) oraz częstość zmiany miejsca pobytu lub pracy.

W tym miejscu rozważań należy także wskazać na pewien trend, który można zauważyć na świecie i który nie dotyczy wyłącznie osób młodych. Chodzi bowiem o przenikanie się czasu wolnego z czasem poświęconym na pracę. Wynika to właśnie z tej wszechogarniającej mobilności i dostępności pewnych usług firmowych, które do tej pory były dostępne tylko w miejscu pracy. Czy sprawdzanie e-maila firmowego po godzinach pracy, czy też na urlopie to już praca? Czy weryfikacja kalendarza firmowego to także praca? Ilekroć zdarzało się nam to robić, bez względu na wiek? Czy w dalszym ciągu traktujemy to jako czynność związaną z pracą? Do tej pory z takim modelem przenikania się życia zawodowego i prywatnego było kojarzone młode pokolenia pracowników – pokolenie Y, które aktywnie wykorzystując nowinki technologiczne, posługuje się mediami i technologiami cyfrowymi. Cechuje je również podejście do pracy zgoła inne niż te, które reprezentowały poprzednie pokolenia. Jego reprezentanci dużą wagę przywiązują do życia prywatnego, oczekując od pracodawcy zapewnienia swobody i elastycznego czasu pracy. Mając duży apetyt na życie, nie chcą go w żaden sposób ograniczać, a już na pewno nie przez pracę. Są postrzegani jako pracownicy nielojalni, którzy nie przywiązują się do firmy i stanowiska i bardzo chętnie się z nią rozstaną, jeśli tylko znajdzie się lepsza praca lub dana firma za bardzo będzie

ingerować w ich życie i swobodę[2]. Biorąc jednak pod uwagę jeszcze jeden element związany z mobilnością, a mianowicie dostępność usług, aplikacji, danych również z prywatnych urządzeń, a nie wyłącznie firmowych, można stwierdzić, że dla nas wszystkich wyrażenie „być w pracy" nabiera zupełnie nowego znaczenia.

Potencjał związany z mobilnością jest możliwy do wykorzystania w dużej mierze dzięki zastosowaniu technologii *cloud computing*, czyli chmury obliczeniowej. Dzięki dynamicznemu rozwojowi tej technologii była możliwa ekspansja w skali świata usług dotąd dostępnych tylko wewnątrz organizacji[3]. Obecnie ponad 31% organizacji w Polsce korzysta z chmury obliczeniowej. Szacuje się, że wartość rynku związanego z tymi usługami w 2019 roku przekroczy 450 mln USD. Bardzo ciekawe jest również to, że migracja do usług w chmurze nie jest silnie skorelowana z branżą, w jakiej działa organizacja, oraz jej wielkością. W badaniach oraz wszelkiego rodzaju raportach migrację tę – poza kwestiami finansowymi oraz technicznymi – uzależnia się od poziomu świadomości użytkowników. Największy przychód i wykorzystanie usług chmurowych jest związane z typem chmury SaaS (*Software as a Service* – 62%), IaaS (*Infrastructure as a Service* – 28%) oraz PaaS (*Platform as a Service* – 10%).

Drugim aspektem, który sprzyja rozwojowi mobilności, jest liczba urządzeń mobilnych oraz coraz bardziej dynamicznie rozwijający się trend pozwalający na wykorzystanie urządzeń prywatnych do pracy zawodowej w organizacji – BYOD (*Bring Your Own Device*). Znacznie przyczyniło się to do wzrostu wykorzystania technologii mobilnych.

Na świecie można obecnie zaobserwować rosnącą tendencję związaną z pracą mobilną oraz mobilnością samych użytkowników. Giganci na rynkach technologicznych, tacy jak Citrix czy też Cisco, przewidują, że prawdziwą przyszłością, w kierunku której będą podążać organizacje, jest mobilny styl pracy oraz wzrost znaczenia mobilności. Tylko w Polsce, jak wynika z badań przeprowadzonych w 2015 roku, jest ponad 19 mln smartfonów[4]. Firma Citrix przewiduje, że do 2020 roku 89% organizacji będzie oferować mobilny styl pracy[5]. Już dziś

---

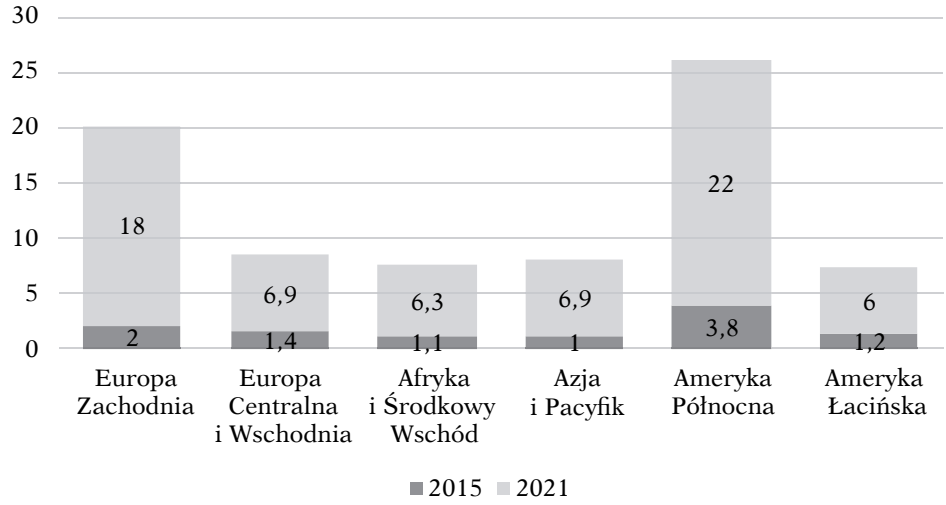
[2] J.A. Fazlagić, *Charakterystyka pokolenia Y*, „e-Mentor" 2008, nr 3(25), http://www.e-mentor.edu.pl/artykul/index/numer/25/id/549 (dostęp: 20.06.2016).

[3] Nie oznacza to oczywiście, że wcześniej dostęp do informacji, pewnych usług czy też aplikacji nie był możliwy. Technologia ta umożliwiła to jednak w większym stopniu, a także pozwoliła ten proces wykorzystać globalnie.

[4] M. Mikowska, *Polska jest Mobi*, http://www.tnsglobal.pl/coslychac/files/2015/05/POLSKA_JEST_MOBI_2015.pdf (dostęp: 20.06.2016).

[5] *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: 20.06.2016).

ilości danych przesyłanych rocznie przez sieci komórkowe są ogromne, a prognoza na lata 2016–2021 wynosi 1600 eksabajtów[6]. Miesięczne wartości transferu danych dla poszczególnych regionów świata ilustruje rysunek 1.



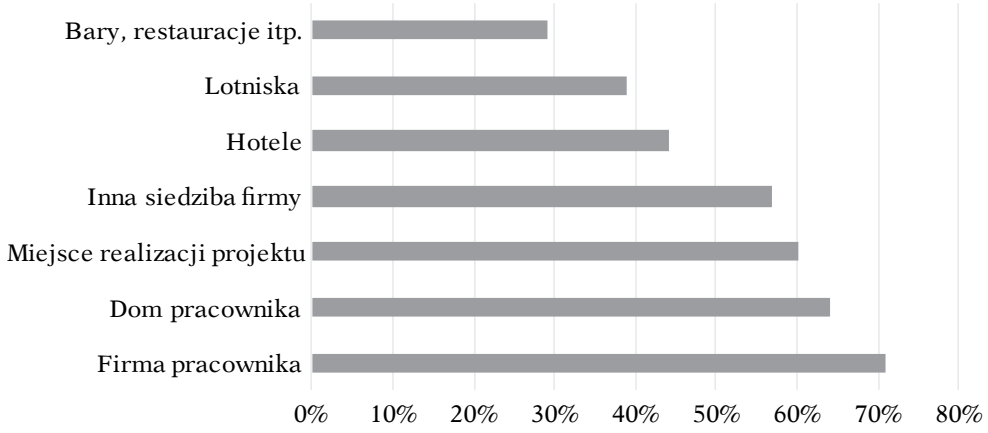
Rysunek 1. Ilość danych przesyłanych miesięcznie z użyciem smartfonów dla wybranych regionów świata z prognozą na lata następne (w GB)

Źródło: opracowanie własne na podstawie: *Ericsson Mobility Report*, http://www.ericsson.com/res/docs/2016/mobility-report/ericsson-mobility-report-feb-2016-interim.pdf (dostęp: 20.06.2016).

Nie należy również zapominać o tym, że wraz ze wzrostem usług mobilnych, dostępności i elastyczności, jaką dają takie rozwiązania, zwiększyły się znacznie wymagania użytkowników dotyczące tychże rozwiązań. Użytkownicy liczą na jak najlepszą jakość oferowanych usług, a także na dostępność o dowolnej porze oraz z dowolnego miejsca na świecie. Sprostanie tym wymaganiom przez organizacje oferujące takie usługi nie jest łatwe. Każdorazowa niedostępność czy też opóźnienie w działaniu samej usługi jest odbierana przez użytkowników bardzo negatywnie i podwyższa poziom ich zestresowania. Firma Ericsson w 2016 roku przeprowadziła badania dotyczące poziomu stresu pojawiającego się w przypadku opóźnienia w działaniu pewnej usługi mobilnej. Z badań tych wynika, że zaobserwowany poziom stresu związany z dwusekundowym opóźnieniem w działaniu usługi mobilnej był porównywalny z poziomem stresu osób oglądających horror czy też rozwiązujących problem matematyczny. Badania

[6] *Ericsson Mobility Report*, http://www.ericsson.com/res/docs/2016/mobility-report/ericsson-mobility-report-feb-2016-interim.pdf (dostęp: 20.06.2016).

te dowodzą, jak ważne dla młodego pokolenia są usługi mobilne i ich niezawodne działanie oraz ich dostępność. Śmiało można powiedzieć, że będzie to także dotyczyło przyszłych pokoleń, które w coraz większym stopniu będą polegać na mobilności dostępu do informacji, usług i aplikacji, a może nawet na mobilności pracy. Wnioski takie potwierdzają już takie firmy jak Ericsson, Citrix czy też Cisco w swoich badaniach i prognozach na przyszłość. Jeśli chodzi o mobilny tryb pracy, Citrix przewiduje zmniejszenie przestrzeni pracowniczej w 2020 roku o 18%[7]. Obecnie większość dużych organizacji w związku ze wzrostem popularności mobilnego stylu pracy oferuje siedem biurek na 10 pracowników i tendencja ta, jak pokazują raporty, jest malejąca. Ogólnoświatowe badania wykazują także, że pracownicy, wykonując swoje czynności zawodowe, coraz częściej korzystają z miejsc do pracy zlokalizowanych poza biurem (rysunek 2).



Rysunek 2. Miejsca aktywności zawodowej pracowników (w %)

Źródło: opracowanie własne na podstawie: *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: 20.06.2016).

Jak widać, tendencje światowe oraz prognozy na lata przyszłe pokazują – czy tego chcemy, czy nie – nieunikniony wzrost znaczenia pracy mobilnej, dostępności usług oraz ogólnie pojętej mobilności użytkowników. Pozostaje tylko zadać sobie jeszcze jedno pytanie: gdzie w tej pogoni za dostępnością i jakością tychże usług ma być umiejscowione bezpieczeństwo?

[7] *Citrix Workplace of the Future*…

3. Bezpieczeństwo informacji w mobilnym środowisku

Bezpieczeństwo informacji zawsze powinno być dla organizacji bardzo istotnym elementem. Element ten okazuje się krytyczny, jeśli chodzi o wszelkie usługi mobilne, które są udostępniane na zewnątrz organizacji. Dotychczas organizacje polegały na zabezpieczeniu dobrze znanych usług, które udostępniały swoim pracownikom na zewnątrz – poczta, wybrane usługi serwerowe (bazy danych, strony WWW). Obecnie ogrom usług, ich dostępności i zróżnicowanie powodują, że odpowiednie zabezpieczenie takiej infrastruktury jest jeszcze trudniejsze. Trudność ta jest także potęgowana w wypadku dostępu z urządzeń mobilnych z powodu zróżnicowania sprzętowego i systemowego.

Większość organizacji, które oferują dostęp mobilny do swoich usług (wszystkich czy też wybranych), ma już odpowiednią do tego infrastrukturę sprzętową. Różnica polega tylko na tym, czy dostęp ten ogranicza się do użytkowników mobilnych wewnątrz organizacji (mobilność użytkowników na poziomie wewnątrzorganizacyjnym), czy też udostępniane usługi są oferowane z dowolnego miejsca na świecie poprzez sieci komórkowe, sieci bezprzewodowe lub połączenia satelitarne. Oferowany przez organizacje dostęp dotyczący tylko wnętrza organizacji, czyli ograniczony obszarowo do jednej lokalizacji geograficznej, jest obecnie najczęściej spotykany. Jest też zazwyczaj możliwy już przez dłuższy okres, stąd można przypuszczać, że w wypadku jego konfiguracji wszelkie mechanizmy zabezpieczające są już dosyć dobrze znane. Nie oznacza to jednak, że jest z nim związany mniejszy poziom zagrożeń na wszelkiego rodzaju ataki. Można tylko uznać, że większość organizacji oferujących taki dostęp użytkownikom mobilnym ma już odpowiednio zdefiniowane procedury, strategie postępowania, jak również wdrożone odpowiednie mechanizmy zabezpieczające. W wypadku dostępu nieograniczającego się do jednej lokalizacji geograficznej skonfigurowanie odpowiednich mechanizmów oraz określenie odpowiednich procedur jest o wiele bardziej trudniejsze.

Utrzymanie odpowiedniego poziomu bezpieczeństwa w środowisku mobilnym może się wiązać również z niemożnością utrzymania pełnej kontroli nad prywatnym urządzeniem mobilnym. Te organizacje, które już wprowadziły mechanizmy ochrony użytkowników mobilnych, mają ułatwiony start, jeśli chodzi o zapewnienie bezpieczeństwa w modelu pracy mobilnej. Istnieje wiele różnic pomiędzy urządzeniami stacjonarnymi, które są w pełni własnością organizacji, a tymi, które są urządzeniami prywatnymi wykorzystywanymi do pracy mobilnej.

Kluczowe dla organizacji zagadnienia związane z kwestiami bezpieczeństwa, a wynikające z pracy mobilnej to:

- identyfikacja urządzeń (*FingerPrinting OS*);
- zarządzanie dostępem do danych;
- ochrona przed wyciekiem danych;
- ochrona danych, aplikacji i usług udostępnianych;
- zarządzanie bezpieczeństwem prywatnych urządzeń mobilnych;
- 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.

Odpowiednie procedury, regulaminy i strategię działania wchodzące w skład PBI powinny określać:

- jakiego typu urządzenia mogą pojawiać się w firmowej sieci (smartfon, tablet, laptop) oraz na jakich zasadach (np. czy potrzebna jest zgoda przełożonego?);
- 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 się w nim 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;

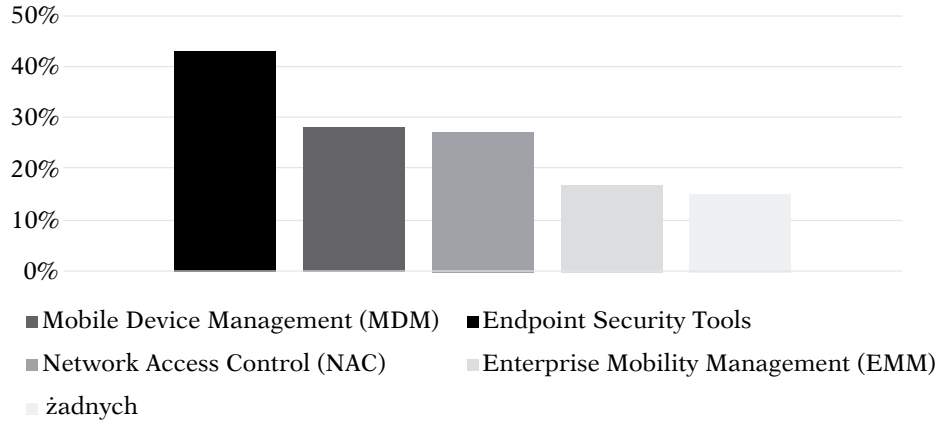
- określenie zasobów, do których będzie konfigurowany dostęp z tychże urządzeń;
- sankcje dyscyplinarne i karne w przypadku naruszenia procedur i/lub zaniedbań ze strony użytkownika.

W wypadku organizacji, która w swoich zasobach posiada dane osobowe i użytkownicy mobilni posiadają dostęp do takich danych, powinny one podlegać innym zasadom ochrony. Wówczas należy ustalić, czy dane osobowe w ogóle mogą być przetwarzane na urządzeniach mobilnych – bez wstępnego rozróżnienia, czy będą to urządzenia prywatne czy firmowe. Jeśli tak, to gdzie dane osobowe mogą być przechowywane i przetwarzane – czy wszystkie typu urządzeń będą miały taką możliwość, jakie warunki muszą spełniać, jakie zabezpieczenia wprowadzone itp. Następnie czy mogą – a jeśli tak, to w jaki sposób – być przenoszone lub przetwarzane na prywatnych urządzeniach mobilnych oraz ewentualnie jakie warunki muszą być ku temu spełnione. Kolejnym krokiem jest określenie, jakie jest ryzyko z tym związane. Szczególnie chodzi o oszacowanie ryzyka związanego z wyciekiem, utratą i kradzieżą takich danych z urządzeń prywatnych. Należałoby także wziąć tutaj pod uwagę ryzyko wykorzystania takich danych przez samego pracownika, na przykład sprzedaż takich danych czy też zabranie ze sobą wraz z odejściem z pracy (np. baza danych klientów, kontrahentów itp.). Jeśli dane osobowe mogą znajdować się na prywatnych urządzeniach mobilnych pracowników, to należy konkretnie zdefiniować (o ile to możliwe) lokalizację takich danych oraz określić, czy dane takie mogą się mieszać z prywatnymi danymi na urządzeniu pracownika.

W celu zapewnienia jak najlepszych mechanizmów zabezpieczających powinno się także określić mechanizmy zabezpieczające urządzenie mobilne. Nie należy także zapominać o zdefiniowaniu i wdrożeniu wszelkich procedur związanych z kasowaniem danych osobowych w kontekście różnych możliwości, począwszy od zerwania umowy z pracownikiem, a kończąc na kradzieży urządzenia. Bardzo ważnym elementem jest procedura związania z serwisowaniem takiego sprzętu, na którym znajdują się bądź znajdowały się jakiekolwiek dane firmowe. Procedura taka powinna określać, jakie czynności powinny być wykonane przed oddaniem urządzenia do serwisu zewnętrznego (np. czyszczenie nośnika danych, wymontowanie nośnika danych itp.) lub wręcz powinny określać – o ile to możliwe – firmy serwisujące, z którymi organizacja ma podpisane stosowne umowy o zachowaniu poufności danych.

Poza odpowiednim podejściem na poziomie wdrożenia PBI organizacja musi także zostać wyposażona w odpowiednią infrastrukturę sprzętowo-narzędziową. Jest ona niezbędnym elementem, który gwarantuje sprawowanie kontroli

nad mobilnym, a także mobilnym i prywatnym środowiskiem pracy, jakie pojawia się w organizacji. Pozwala ona 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. Dlatego też elementem składowym, bez którego nie ma mowy o BYOD, są aplikacje typu MDM (ang. *Mobile Device Management*). Oprogramowanie to umożliwia wszechstronne zarządzanie oraz monitorowanie mobilnych urządzeń, które mają dostęp do poufnych danych i usług. Coraz częściej aplikacje tego typu są rozszerzane o aplikację typu MAM (ang. *Mobile Application Management*) oraz MCM (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. Zasady działania tego typu oprogramowania są w zależności od producenta minimalnie różne, natomiast 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 od firmy. Typy narzędzi, które wykorzystują organizacje, przedstawia rysunek 3.



Rysunek 3. Typy narzędzi wykorzystywanych przez organizację w wypadku mobilnego typu pracy (w %)

Źródło: opracowanie własne na podstawie: *BYOD & Mobile Security 2016*, www.gyartastrend.hu/download.php?id=27070 (dostęp: 20.06.2016).

Jak widać, zapewnienie odpowiedniego poziomu bezpieczeństwa w wypadku mobilnego środowiska pracy nie jest zadaniem łatwym ze względu na wiele wiążących się z tym aspektów. Jednak odpowiednio zaplanowane wdrożenie takiego środowiska, usług, procedur oraz dobrze opracowana PBI pozwala podjąć to nowe wyzwanie. Na pewno wymaga to stworzenia lub zmodyfikowania już istniejących strategii dotyczących infrastruktury IT, jak również całej organizacji. Dużym wyzwaniem może być kontrola przepływu danych w urządzeniach mobilnych. Natomiast dzięki takim rozwiązaniom jak konteneryzacja, zapewniająca oddzielenie danych firmowych od prywatnych, szyfrowanie czy też podnoszenie poziomu świadomości użytkowników poprzez szkolenia oraz infrastruktura MDM prawie każda organizacja może wdrożyć model pracy mobilnej – choć na pewno nie będzie to proces łatwy ani tani. Jednak korzyści wynikające ze zwiększonej produktywności użytkowników, ich zadowolenie oraz zyski finansowe powinny zrównoważyć lub nawet przewyższyć koszty.

4. Podsumowanie

Kluczowym elementem dla każdej organizacji jest utrzymanie odpowiedniego poziomu bezpieczeństwa informacji. W świecie opartym na technologiach teleinformatycznych jest to zagadnienie niezwykle istotne i bardzo trudne. Mając na uwadze wszelkie prognozy i statystyki dotyczące modelu pracy mobilnej oraz mobilności użytkowników, można stwierdzić, że wydaje się on naturalnym etapem rozwoju obecnego świata 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 na kompleksowe wdrożenie modelu BYOD, dzięki któremu pracownicy mogą korzystać ze swoich prywatnych urządzeń, wykonując codzienne obowiązki. Jeśli jest to działalność świadoma, wówczas można liczyć na większy poziom bezpieczeństwa, który może organizacja zapewnić, oraz na korzyści finansowe i personalne. Nieświadoma zgoda na tego typu praktyki związane z korzystaniem z prywatnych urządzeń w organizacji spowoduje niestety porażkę zarówno pod względem bezpieczeństwa informacji, jak i korzyści finansowych związanych z tego typu rozwiązaniem. Należy pamiętać, że niemożliwe jest osiągnięcie 100-procentowego poziomu bezpieczeństwa. Można jednak, stosując odpowiednie procedury, strategie oraz mechanizmy zabezpieczeń,

zmniejszyć ryzyko wystąpienia zagrożeń, a przez to zapewnić odpowiedni poziom bezpieczeństwa informacji. Mobilność użytkowników w organizacji, a co za tym idzie – dostępność usług i informacji, jest swoistym wyzwaniem dla organizacji. Wraz z niemałymi korzyściami pojawiają się nowe, niemałe wyzwania. Oprócz bezpieczeństwa istnieje wiele problemów związanych z aspektami prawnymi, kosztami oraz prywatnością, które każda organizacja musi wziąć pod uwagę. Bardzo często niestety za dynamicznie rozwijającymi się technologiami i nowymi możliwościami nie nadążają regulacje prawne. Jest tak też w wypadku mobilności użytkowników w miejscu pracy czy też mobilności w dostępie do usług i informacji udostępnianych przez organizacje.

Bibliografia

Dirk N., *Mobile Strategy: How Your Company Can Win by Embracing Mobile Technologies*, IBM Press, Indianapolis 2013.

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

Patel R., *Enterprise Mobility Strategy&Solutions*, Wyd. Partridge India, India 2014.

Źródła sieciowe

BYOD & Mobile Security 2016, www.gyartastrend.hu/download.php?id=27070 (dostęp: 20.06.2016).

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: 20.06.2016).

Ericsson Mobility Report, http://www.ericsson.com/res/docs/2016/mobility-report/ericsson-mobility-report-feb-2016-interim.pdf (dostęp: 20.06.2016).

Fazlagić J.A., *Charakterystyka pokolenia Y*, „e-Mentor" 2008, nr 3(25), http://www.e-mentor.edu.pl/artykul/index/numer/25/id/549 (dostęp: 20.06.2016).

http://www.outsourcingportal.eu/pl/userfiles/image/raporty/2014/02_lut/25/Branza_Teleinformatyczna_Trendy_i_Wyzwania.pdf (dostęp: 20.06.2016).

Mikowska M., *Polska jest Mobi*, http://www.tnsglobal.pl/coslychac/files/2015/05/POLSKA_JEST_MOBI_2015.pdf (dostęp: 20.06.2016).

* * *

Mobility of Users and Information Security in the IT Environment

Summary

Mobility of users is becoming commonplace for many modern organizations. The impact of this mobile work is not limited only to IT departments, but has also moved to other areas of the organization. Like any new trend, it brings with it many benefits for both the organization and employees, as well as many hazards and problems. The aim of the author is to discuss the possibilities for the modern organization which goes in the direction of mobile working. The author shows how the approach is changing to the management of the institution to the network, mobile devices, to information security as well as the workers themselves, for whom the phrase "be at work" takes on a new meaning.

Keywords: users' mobility, security, data security, BYOD.