Zeszyty Naukowe Politechniki Częstochowskiej
Zarządzanie Nr 31 (2018) s. 7-16
dostępne na: http://www.wz.pcz.pl/znwz

BYOD JAKO ZNACZĄCY ELEMENT RYZYKA OPERACYJNEGO PRZEDSIĘBIORSTWA

Jacek Chmielewski

Politechnika Częstochowska
Wydział Zarządzania
(uczestnik studiów doktoranckich)

Streszczenie: Artykuł w głównej mierze poświęcony jest problematyce wykorzystywania w organizacjach trendu BYOD (*Bring Your Own Device*), czyli polityce przedsiębiorstwa zezwalającej pracownikom na wykorzystywanie ich prywatnych urządzeń mobilnych do wykonywania obowiązków zawodowych, w tym na dostęp do zasobów firmowych (https://securelist.com/…). Przedstawia zalety oraz wady koncepcji związane z implementacją rozwiązania w strukturach podmiotu. Stara się także nakreślić wymiar ryzyka, jakie niesie wdrożenie modelu BYOD, w szczególności – jak odnosi się do poziomu ryzyka operacyjnego ponoszonego przez firmę. Nakreśla mapę zagrożeń oraz wektory ich oddziaływań na przedsiębiorstwo. Wskazuje główne metody pozwalające na minimalizację niebezpieczeństw wynikających z trendu BYOD, odpowiada na pytania o bezpieczeństwo informatyczne organizacji, które zaimplementowały rozwiązanie wewnątrz własnej struktury.

Słowa kluczowe: BYOD, konsumeryzacja, ryzyko operacyjne, zagrożenia, bezpieczeństwo, kadra

DOI: 10.17512/znpcz.2018.3.01

Wprowadzenie

Obecnie coraz trudniejszym zadaniem staje się wskazanie przedsiębiorstwa, które nie korzysta z jakiegokolwiek narzędzia informatycznego. Komputery, tablety, smartfony, GPS, dedykowane oprogramowanie i usługi, szybkie łącza oraz nowe kanały komunikacji – to środki, które pozwalają zwiększyć efektywność firm oraz zredukować koszty ich działalności. Rynek rozwiązań IT i związany z nim popyt na urządzenia i oprogramowanie informatyczne sprawił, że producenci zmuszeni zostali nie tylko do obniżenia cen, ale także do oferowania bardziej zaawansowanych funkcjonalności i lepszego wsparcia klienta. Paradoksalnie szeroki wybór opcji wraz z niewłaściwym rozpoznaniem własnych potrzeb powoduje, że niektóre z podmiotów nie są w stanie wybrać najkorzystniejszego rozwiązania. Większość z przedsiębiorstw poprawnie rozpoznaje własne potrzeby i sprawnie asymiluje technologiczne nowości na potrzeby działalności. Obserwują także środowisko własnego personelu w poszukiwaniu wskazówek dotyczących wyboru właściwego sprzętu czy oprogramowania. Często właśnie pracownicy wskazują, jakie urządzenia i aplikacje konsumenckie (Jędrzejczyk 2015, s. 84) są im potrzebne. Dzieje się to zarówno na drodze formalnej, polegającej na raportowaniu przez

kadrę potrzeb, jak i nieformalnej, skupiającej się na obserwowaniu działań pracowników i przyglądaniu się, które z ich prywatnych narzędzi są wykorzystywane zawodowo. Drugi z przypadków może budzić kontrowersje. Jeśli korzystanie z prywatnych urządzeń wpływa na zwiększanie produktywności pracownika lub przyczynia się do oszczędności wynikających z tytułu zakupu sprzętu, to utrzymanie takiego stanu powinno leżeć w interesie przedsiębiorstwa. Mając jednak na uwadze ochronę zasobów firmy, każde prywatne urządzenie czy aplikacja, które działają na styku z infrastrukturą IT przedsiębiorstwa, są potencjalnym zagrożeniem, a ich wykorzystanie powinno być penalizowane. Zjawisko wykorzystywania w pracy prywatnych urządzeń (w większości mobilnych), określane jako konsumeryzacja w IT lub nazwane z angielskiego *Bring Your Own Device* (BYOD), staje się nieodłącznym elementem funkcjonowania współczesnych organizacji i nie jest już rozwijającym się trendem, ale powszechnie stosowaną praktyką biznesową (https://www.kaspersky.pl/…). Według badań przeprowadzonych w 2016 roku przez firmę Syntonic Inc. na rynku amerykańskim aż 59% przedsiębiorstw, które zatrudniają nie mniej niż 100 pracowników, wprowadziło już formalnie programy wspierające BYOD (https://syntonic.com/…). Z kolei według analiz przeprowadzonych przez Kaspersky Lab wynika, że aż 62% właścicieli i pracowników wykorzystuje prywatne urządzenia mobilne w pracy (https://www.kaspersky.pl/…). Zgodnie z wynikami europejskich badań, które zostały zlecone przez firmę Microsoft (https://news.microsoft.com/…), najczęściej wybieranymi przez pracowników prywatnymi urządzeniami do pracy są laptopy (57%), w dalszej kolejności telefony komórkowe (55%), smartfony (52%) i tablety (22%), a zatem przede wszystkim urządzenia mobilne. Za popularyzacją BYOD stoi prężny rozwój rynku urządzeń mobilnych, upowszechnienie się szybkich bezprzewodowych kanałów dostępowych do sieci Internet oraz rosnąca popularność rozwiązań chmurowych i komunikacyjnych. Katalizatorem rozwoju BYOD jest także chęć bycia online przez pracowników – czyli możliwość korzystania z dostępu do sieci w dowolnej chwili, śledzenia mediów społecznościowych, komentowania wydarzeń, komunikowania się czy wymiany treści. Istotna jest także postawa pracodawców, którzy w realiach rynku pracy (rynek pracownika) skłonni są do oferowania kandydatom dodatkowych profitów oraz liberalizacji niektórych zasad – np. dotyczących korzystania w trakcie pracy z portali społecznościowych czy komunikatorów.

Przedsiębiorstwa coraz częściej stają przed dylematem, czy podążać za trendami rynkowymi, jak BYOD, czy pozostać w nurcie konserwatywnym, będącym sceptycznym wobec radykalnych zmian? BYOD mimo swoich zalet z pewnością pociąga za sobą pewnego rodzaju liberalizację zasad i reguł panujących w firmie, co przekłada się na wzrost ryzyka operacyjnego dla podmiotu.

Głównym celem artykułu jest wskazanie zagrożeń związanych z wdrożeniem trendu konsumeryzacji w kontekście ryzyka operacyjnego ponoszonego przez przedsiębiorstwo. Badania zostały przeprowadzone w oparciu o analizę wtórną danych opracowanych przez organizacje zajmujące się bezpieczeństwem informatycznym oraz informacje zawarte w literaturze tematycznej.

BYOD – szanse i zagrożenia

Konsumeryzacja stała się powszechnym zjawiskiem, które na stałe wpisało się w funkcjonowanie organizacji działających na całym świecie. W zależności od regionu stopień implementacji trendu jest zróżnicowany. Większy odsetek przedsiębiorstw, które zaabsorbowały model BYOD, występuje w krajach wysoko rozwiniętych lub rozwiniętych, mniejszy wśród rynków wschodzących. W Polsce, zdaniem dostawców rozwiązań IT, można mówić jeszcze o małym zainteresowaniu trendem i wolniejszym jego rozwoju niż w przypadku krajów Europy Zachodniej (Jaślan 2016, s. 32). Analizując tendencje rozwojowe technologii IT, jakie pojawiły się na rynkach zachodnioeuropejskich czy amerykańskim w ostatniej dekadzie, oraz czas, po którym przyjęły się na polskim rynku, można założyć, że konsumeryzacja w IT zostanie niebawem mocno osadzona w realiach polskiego biznesu. Fakt, że Polska nie jest w czołówce krajów, które posiadają największy odsetek firm korzystających z trendu, BYOD może mieć swoje zalety. Obserwując liderów, można wyciągnąć wnioski oparte na empirycznych doświadczeniach poprzedników, które być może pozwolą uniknąć błędów, na które narażeni byli prekursorzy. Daje to także okoliczność do weryfikacji faktycznych zalet konsumeryzacji i szansę maksymalizacji korzyści z niej płynących. Istotną kwestią jest pytanie o korzyści wdrożenia modelu BYOD w przedsiębiorstwie i jego negatywne aspekty. Wśród oczywistych zalet trendu wymienia się przede wszystkim obniżenie kosztów związanych z zakupem sprzętu i oprogramowania, wzrost elastyczności związanej z faktem, iż pracownik przez większość czasu nie rozstaje się z własnym urządzeniem, gdziekolwiek się znajduje, a także coraz istotniejsza staje się kwestia dobrego morale załogi, które pośrednio wpływa na produktywność. Wśród benefitów wymienić należy także wzrost mobilności, oszczędność czasu pracowników czy fakt, że pracują na swoim dobrze znanym im sprzęcie i oprogramowaniu (Portela, Moreira da Vega, Santos 2018, s. 38), co przyczynia się do wzrostu ich efektywności.

BYOD posiada także wady, które w wyraźny sposób stają w opozycji do opisanych powyżej korzyści. Jakie ryzyko niesie zatem implementacja trendu konsumeryzacji? Dla większości oficerów bezpieczeństwa zajmujących się ochroną infrastruktury informatycznej – w tym ochroną informacji – wdrożenie polityki BYOD kojarzy się z poważnym wyzwaniem dotyczącym zabezpieczenia wewnętrznych zasobów IT firmy. BYOD generuje przyrost użycia prywatnych urządzeń (Kobis 2017, s. 189) wewnątrz sieci firmowej, co implikuje powstanie wielu zagrożeń. W pierwszej kolejności należy wymienić brak wystarczającej wiedzy na temat środowisk, z których korzystają pracownicy, informacji na temat zainstalowanych aplikacji (często niecertyfikowanych), danych na temat rodzaju informacji, jakie przechowują, czy sposobu ich wymiany. Duże znaczenie ma także metoda ochrony urządzeń należących do pracowników, fakt, czy posiadają zabezpieczenia w postaci pakietu antywirusowego, czy dostęp do nich chroniony jest hasłem lub zabezpieczeniem biometrycznym, czy sprzęt posiada aktywne funkcje pozwalające na lokalizację i zdalne zablokowanie lub usunięcie danych w przypadku jego kradzieży lub zgubienia. Oprócz aspektów technicznych ważny dla administratorów jest sto-

pień świadomości personelu na temat niebezpieczeństw związanych ze zjawiskiem BYOD. Niewystarczająco wyedukowany personel znacząco przyczynia się do obniżenia poziomu ochrony infrastruktury, a co za tym idzie – może generować incydenty bezpieczeństwa. Niebagatelny wpływ ma także fakt istnienia ogromnej liczby cyberzagrożeń, których oddziaływanie przejawia się nie tylko w postaci infekcji systemów, ale także poprzez inwigilowanie użytkowników, kradzież ich danych czy nawet tożsamości. Obawy o bezpieczeństwo potwierdzają firmy z branży bezpieczeństwa. Według Kaspersky Lab 58% właścicieli dużych firm obawia się zgubienia lub kradzieży urządzeń pracowników (a zatem danych na nich zapisanych, a często także punktów dostępowych do infrastruktury przedsiębiorstwa) (https://www.kaspersky.pl/…). Z kolei jak informuje Trend Micro, ponad 46% firm pozwalających pracownikom na korzystanie z własnych urządzeń spotkało się z naruszeniem bezpieczeństwa danych (https://www.trendmicro.com/…). Utrata danych, nieautoryzowany dostęp do zasobów firmy, infekcje złośliwym oprogramowaniem (*malware*), nadużycia, wyłudzenia czy wspomniane kradzieże urządzeń – to jedynie przykłady zagrożeń, które mogą być intensyfikowane w sytuacji wdrożenia polityki BYOD.

Problematyka zagrożeń informatycznych jest jednym z często poruszanych aspektów BYOD, ale nie jedynym. Uwagi wymagają także uwarunkowania prawne i fiskalne. Pierwsze z nich dotyczą kwestii np. licencjonowania oprogramowania, które używane jest w ramach BYOD, czy choćby przechowywania czy przetwarzania danych firmowych zapisanych na sprzęcie pracowników. Producenci oprogramowania często rozróżniają swoje produkty na te do użytku domowego i te, których przeznaczeniem jest użytek komercyjny. Problem pojawia się w sytuacji, kiedy pracownik korzystający z własnego sprzętu i oprogramowania wykonuje czynności firmowe. Jeśli korzysta z oprogramowania nieprzeznaczonego do użytku komercyjnego, to czy łamie zapisy umowy licencyjnej (*End User Licence Agreement*), czy też nie? Jeśli łamie, to czy firma powinna ponieść ewentualne konsekwencje prawne pogwałcenia zapisów umowy? Problemem jest także jasna interpretacja przepisów prawa podatkowego lub jego braki w zakresie pojawiających się nowych zjawisk, takich jak BYOD. Za przykład może posłużyć interpretacja użytkowania prywatnego urządzenia pracownika w celach związanych z wykonywaniem pracy. Czy fakt ten stanowi nieodpłatne świadczenie usługi na rzecz pracodawcy, które podlega opodatkowaniu jako jego przychód, czy jednak nie (http://ksiegowosc.infor.pl/…).

Tabela 1. Zalety i wady trendu Bring Your Own Device

Zalety	Wady
• redukcja kosztów związanych z zakupem sprzętu/oprogramowania dla pracowników • wzrost elastyczności • zwiększenie produktywności • podniesienie morale załogi • większa mobilność pracowników (a także ich dostępność)	• zagrożenia związane z bezpieczeństwem informatycznym zasobów firmy: ⇒ infekcja zasobów poprzez *malware* ⇒ nieautoryzowany dostęp osób trzecich do infrastruktury IT ⇒ brak zabezpieczeń urządzeń (pakiety AV, hasła dostępowe, zabezpieczenia

• oszczędność czasu pracowników • dogodne środowiska IT pracy (lepsza znajomość własnych urządzeń i oprogramowania)	biometryczne) ⇒ wyciek danych (*data leakage*) ⇒ możliwość zgubienia lub kradzieży urządzenia (posiadającego dostęp do zasobów / zapisane newralgiczne dane) ⇒ brak lub niedostateczna wiedza na temat aplikacji instalowanych przez pracowników ⇒ problemy aktualizacji aplikacji i systemów operacyjnych urządzeń (łatki) ⇒ heterogeniczne środowisko IT, trudne do zabezpieczenia (wiele systemów, różnorodność urządzeń) ⇒ edukacja personelu na temat zagrożeń IT ⇒ złudna świadomość pracowników o bezpieczeństwie ich urządzeń • brak wyraźnej granicy pomiędzy strefą prywatną a służbową • implikacje prawne związane z licencjonowaniem oprogramowania (użytek domowy a komercyjny) • zagrożenia związane z prawem podatkowym

Źródło: Opracowanie własne

Dokładne zgłębienie problematyki korzyści i wad wprowadzenia trendu BYOD z pewnością wymaga szerszego spojrzenia i analizy. Autor skupił się wyłącznie na najważniejszych z nich, które podsumowane zostały w *Tabeli 1*.

BYOD jako element ryzyka operacyjnego

Jedna z wielu definicji ryzyka określa je jako niebezpieczeństwo, że coś zdarzy się w inny od oczekiwanego sposób (https://sjp.pl/…). Skupia się wokół niepewności co do rezultatu podjętych decyzji czy przeprowadzonych działań. W literaturze poświęconej zarządzaniu słowo „ryzyko" głównie wiązane jest z szeroko rozumianymi zagrożeniami dla prowadzenia działalności. Dokonuje się także jego klasyfikacji według wielu kryteriów, dzieląc je na poszczególne grupy. Jednym z rodzajów ryzyka obejmującym zagadnienia związane z niebezpieczeństwami generowanymi przez użytkowanie systemów informatycznych, urządzeń oraz występowaniem czynnika ludzkiego jest ryzyko operacyjne. Charakterystyka trendu BYOD wyraźnie wskazuje, że ryzyka związane z jego implementacją będą zawierać się właśnie w zakresie ryzyka operacyjnego. Wynika to z faktu, iż ewentualne starty, które może ponieść podmiot, generowane są przez niedoskonałość infrastruktury informatycznej (systemy i urządzenia) oraz przez działalność pracowników. Wska-

zuje na to sama definicja ryzyka operacyjnego, która określa je jako ryzyko poniesienia strat w wyniku działania niesprawnych systemów, niewystarczającej kontroli, błędów człowieka lub niewłaściwego zarządzania (Tarczyński, Mojsiewicz 2001, s. 22). Podjęcie decyzji przedsiębiorstwa o wprowadzeniu trendu BYOD obarczone jest sporym ryzykiem. Niepewność wynikająca ze swobodnych zachowań pracowników, które dotyczą wykorzystania własnych urządzeń w połączeniu z ich dostępem do zasobów firmy, musi generować powstawanie ryzyka operacyjnego dla podmiotu. Próba ucieczki przed nowymi technologiami nie jest żadnym rozwiązaniem. Dominujący nurt szeroko pojętej informatyzacji sprawia, że wyłącznie firmy korzystające z nowoczesnych technologii mogą być konkurencyjne na rynku. Niestety dla większości firm wzrastające uzależnienie od technologii informatycznych zmusza je do poświęcania coraz większej uwagi konieczności zapewnienia bezpieczeństwa własnych zasobów. Ewolucja zagrożeń jako nierozłączny element rozwoju technologii zmusza do inwestowania znacznych kwot pieniędzy przeznaczonych na środki ochrony (sprzęt, oprogramowanie), poświęcania czasu oraz zasobów ludzkich do przeciwstawienia się niebezpieczeństwom, które z roku na rok przyczyniają się do powstawiania ogromnych start finansowych czy reputacyjnych. Wdrożone środki przeciwdziałania zagrożeniom przyczyniają się automatycznie do redukcji ryzyka wynikającego z funkcjonowania infrastruktury IT, ale zwiększają ryzyko finansowe. W przypadku stacjonarnych zasobów IT wdrożenie właściwych polityk i środków zaradczych jest prostsze niż w przypadku ich mobilnych elementów. Obecnie urządzenia przenośne są najbardziej krytycznym elementem cyberbezpieczeństwa przedsiębiorstw (Jaślan 2017, s. 50), generującym znaczącą część wszystkich incydentów bezpieczeństwa. Rozpatrując trend konsumeryzacji z punktu widzenia ponoszonego ryzyka, można dokonać ich przykładowego podziału na ryzyka oddziałujące bezpośrednio oraz pośrednio. Pierwsza z grup dotyczy wszelkiego ryzyka, które w sposób bezpośredni zagraża funkcjonowaniu organizacji, druga z grup skupia w sobie ryzyka będące pochodną ryzyka bezpośredniego, którego skutki w sposób pośredni oddziałują na procesy zachodzące w przedsiębiorstwie. Ryzyka bezpośrednie w głównej mierze skupiają się wokół technicznych aspektów zjawiska BYOD, dotyczą np. ryzyka zainfekowania urządzenia pracownika szkodliwym oprogramowaniem (pobieranie i instalowanie niecertyfikowanego oprogramowania, odwiedzanie niebezpiecznych stron WWW, podłączanie urządzeń do niezabezpieczonych sieci etc.), uzyskania nieautoryzowanego dostępu do zasobów firmy przez osoby trzecie, ryzyka wycieku danych w przypadku kradzieży bądź zagubienia urządzenia, ryzyka inwigilacji firmy poprzez oprogramowanie szpiegujące zainstalowane nieświadomie przez zatrudnionego. W drugiej z grup znajdują się ryzyka związane z kwestiami prawnymi wykorzystania oprogramowania zainstalowanego na prywatnych urządzeniach (w przypadku, gdy licencja nie zezwala na komercyjny użytek), ryzyko fiskalne, ryzyko utraty reputacji (zgubienie np. laptopa z danymi klienta czy poufną umową) czy ryzyko upublicznienia danych (np. przypadkowe wysłanie wiadomości do niewłaściwego adresata). Konsumeryzacja niesie także ryzyko poniesienia kosztów ochrony własnej infrastruktury, co może znacząco wpływać na opłacalność realizacji przedsięwzięcia. Paradoksalnie także przeciwnicy implementacji BYOD ponoszą ryzyko.

W głównej mierze związane jest to z problemem ewentualnych strat w produktywności (mogą nie skorzystać ze wzrostu efektywności pracowników, który dałoby wprowadzenie BYOD, a zatem ponoszą ryzyko starty). Podejmowanie ryzyka oznacza podejmowanie trudnych decyzji (Griffin 2017, s. 90). W przypadku BYOD bilans zysku i start może być różny. Wynika to z kombinacji wielu czynników. Trend rynkowy wskazuje, że konsumeryzacja w IT będzie postępować, a przed wspomnianą decyzją prędzej czy później stanie większość z włodarzy firm. Decyzja co do sensowności wprowadzenia modelu konsumeryzacji musi zostać poprzedzona szerszą analizą całości zagadnienia, obejmującą bilans zysku i strat implementacji rozwiązania, analizę bezpieczeństwa wewnętrznych zasobów informatycznych firmy, zawierającą także media komunikacyjne i formy łączności czy analizę dotyczącą możliwości ochrony punktów dostępowych. Weryfikacji wymagać będą także aspekty finansowe, prawne i fiskalne. Pomoże to w przyszłości uniknąć implikacji prawno-podatkowych. Oczywistym wydaje się też zapytanie pracowników o chęć uczestnictwa w takim modelu biznesowym, gdyż forsowanie zmian może nie przynieść zamierzonego efektu. Wprowadzenie modelu BYOD nie jest zadaniem trywialnym i z pewnością obarczone jest dużą dozą niepewności, a co za tym idzie – ryzyka dla podmiotu.

Przeciwdziałanie zagrożeniom

Głównym problemem modelu BYOD jest brak kontroli firmy nad urządzeniami pracowników. Zasoby zlokalizowane wewnątrz firmy z reguły są chronione przez administratorów za pomocą oprogramowania zabezpieczającego, firewalli, poprzez urządzenia typu „*appliance*" czy nadawanie właściwych uprawnień i ograniczanie dostępu do określonych zasobów. Wykorzystują także dedykowane narzędzia informatyczne służące do szyfrowania danych, tunelowania transmisji czy duplikowania zasobów. Mają również szerokie możliwości wymuszania na użytkownikach sprzętu i oprogramowania określonych zachowań, np. okresowej zmiany haseł czy aktualizacji systemów operacyjnych i aplikacji. Wdrażają także odpowiednią politykę bezpieczeństwa (Kiełtyka 2017, s. 103), która definiuje zasady, procedury oraz środki niezbędne do ochrony zasobów. Daje to możliwość kontrolowania infrastruktury IT oraz zapobiegania występowaniu incydentów bezpieczeństwa. Niestety urządzenia, które należą do pracowników i są przez nich wykorzystywane w pracy, nie podlegają takim restrykcjom, jak te będące własnością firmy. Stanowią słabe elementy łańcucha bezpieczeństwa, podobnie zresztą jak ich użytkownicy. Właściwą drogą jest zadbanie o zabezpieczenie urządzeń pracowników, a także o ich edukowanie. Trend BYOD nie przeszedł niezauważony przez dostawców rozwiązań dla branży IT, którzy oferują dedykowane rozwiązania do zarządzania i ochrony urządzeń mobilnych określane jako MDM (*Mobile Device Management*) (https://www.pcmag.com/…). Obecnie wspierają większość popularnych platform mobilnych, takich jak Android, iOS, Windows czy Blackberry. Zakres oferowanych opcji jest zróżnicowany; wśród głównych funkcji można wymienić separację danych firmowych i prywatnych, lokalizację urządzeń, zdalne usuwanie danych (także granularne), tworzenie kopii danych na serwerach czy możliwość tunelowa-

nia łączy. Niestety pełne wykorzystanie możliwości MDM jest zależne od zgody pracownika na zainstalowanie elementów MDM na jego urządzeniu. Jest to kwestia problematyczna z wielu powodów, począwszy od spraw związanych z prywatnością użytkownika (oddzielenie sfery prywatnej od zawodowej), przez zakres wpływu rozwiązania na urządzenie, po kwestie ewentualnych akcji wykonywanych na urządzeniu. Z tych powodów część firm nie decyduje się na wdrożenie MDM i szuka innych rozwiązań, które pozwolą korzystać z zalet modelu BYOD. Te, które zdecydują się na MDM, staną przed faktem konieczności uregulowania aspektów prywatności pracowników. Wskazanym jest wykorzystanie dróg formalnych np. sporządzenie odpowiedniej umowy. Rozwiązania *Mobile Device Management* pokrywają jedynie część obszaru zabezpieczanego przez rozwiązania klasy EMM (*Enterprise Mobility Management*), które oprócz zarządzania i ochrony urządzeń oferuje kontrolę nad szeregiem dodatkowych usług. Dużą zaletą rozwiązań EMM jest ich skalowalność i zakres oferowanej ochrony, niestety podobnie jak w przypadku MDM, aby spełniały swoją rolę, wymagana jest pełna integracja urządzeń z infrastrukturą firmy.

Oprócz rozwiązań klasy MDM czy EMM wdrażane są także narzędzia pozwalające na zdalny dostęp do zasobów z wykorzystaniem bezpiecznych łączy tunelowanych (VPN – *Virtual Private Network*) oraz poświadczeń (certyfikatów) nadanych przez administratorów, przy czym nie wymagają one instalowania aplikacji, które ingerują w prywatność użytkownika. Umożliwiają zestawienie bezpiecznego połączenia urządzenia z zasobami firmy, ale niestety nie ustrzegą przed infekcją złośliwym oprogramowaniem. Dlatego w interesie firmy leży zachęcanie użytkowników do korzystania z pakietów bezpieczeństwa chroniących przed złośliwym oprogramowaniem, phisingiem czy kradzieżą danych. Jednym z rozwiązań uzupełniających jest także limitowanie dostępu do zasobów. Wymaga to jednak przeprowadzenia dogłębnej analizy, gdyż zbyt restrykcyjne podejście do kwestii dostępów może prowadzić do bezzasadności wykorzystania zalet mobilności. Z kolei polityka „szeroko otwartych drzwi" rodzi problem ewentualnych nadużyć związanych z wyciekiem danych. Bardzo dobrą praktyką jest edukowanie personelu, czyli budowanie świadomości występowania zagrożeń, wektorów ich oddziaływania oraz skutków, jakie mogą wywołać. Użytkownik, który nie jest świadomy istnienia zagrożeń, nie będzie mógł ich rozpoznać i zareagować w pożądany sposób (Chmielewski 2017, s. 82), zatem przyczyni się do powstania incydentu bezpieczeństwa. W trakcie szkoleń załoga powinna zostać zapoznana z polityką bezpieczeństwa firmy, a przynajmniej z częścią poświęconą ochronie zasobów przedsiębiorstwa i regulacjom dotyczącym personelu. Pożądaną cechą szkoleń jest ich cykliczność, która pozwala na regularne monitowanie personelu o aktualnych zagrożeniach oraz informowanie o ewentualnych zmianach w polityce bezpieczeństwa firmy.

Artykuł niniejszy nakreślił jedynie ogólne możliwości przeciwdziałania zagrożeniom wynikającym z charakterystyki modelu *Bring You Own Device*. Zbudowanie efektywnego rozwiązania zabezpieczającego zasoby przedsiębiorstwa wymagać będzie gruntownych analiz zagrożeń, rozpoznania rynku oferentów dedykowanych rozwiązań oraz stworzenia odpowiednich polityk i regulacji wewnątrzzakładowych.

Podsumowanie

Trend BYOD z roku na rok zdobywa coraz więcej zwolenników i staje się powszechną praktyką biznesową. Powodem jest konwergencja interesów przedsiębiorstw i ich pracowników.

Wzrost produktywności, elastyczność i redukcja kosztów organizacji to najważniejsze z korzyści konsumeryzacji. Kosztem ponoszonym przez firmy, które implementują BYOD, jest wzrost poziomu ryzyka operacyjnego. W głównej mierze dotyczy to ryzyka utarty danych lub możliwości ich upublicznienia, infekcji zasobów informatycznych złośliwym oprogramowywaniem czy zyskaniem nieautoryzowanego dostępu do infrastruktury IT firmy przez osoby trzecie. Zagrożenia te mogą w istotny sposób wpłynąć na prawidłowość procesów zachodzących w przedsiębiorstwie, zaburzając lub uniemożliwiając sprawne funkcjonowanie podmiotu. Podmioty planujące wdrożyć BYOD powinny przeprowadzić analizy bezpieczeństwa własnej infrastruktury informatycznej i na podstawie wyników zastosować niezbędne środki zapobiegawcze w postaci dedykowanych aplikacji zabezpieczających czy poprzez edukowanie personelu. W przypadku gdy firma nie posiada wystarczających kompetencji w zakresie przeprowadzenia badań poziomu ochrony lub środków technicznych, takie analizy może zlecić zewnętrznym firmom informatycznym wyspecjalizowanym w testach penetracyjnych infrastruktury IT. Negatywną stroną wprowadzenia modelu BYOD jest także konieczność weryfikacji jego zagadnień fiskalno-prawnych, które w połączeniu z brakiem lub niedokładnością odpowiednich przepisów podatkowych i regulacji mogą implikować dodatkowe ryzyka (związane jest to w dużej mierze ze swobodą interpretacji zapisów ustaw lub ich brakiem). Także i w tym przypadku najlepszą z dróg będzie przeprowadzenie własnych analiz lub skorzystanie z doświadczenia kancelarii prawnych i podatkowych specjalizujących się w zagadnieniach konsumeryzacji. Wdrożenie BYOD to także większe ryzyko utraty reputacji firmy, która na współczesnym rynku jest jednym z czynników pozwalających efektywnie konkurować z innymi przedsiębiorstwami. Sprawne zapobieganie utracie dobrego imienia wiąże się z uruchomieniem i kolektywnym działaniem wszelkich możliwych środków ochrony, zarówno tych technicznych, jak i prawnych. Konsumeryzacja z pewnością wymaga zastosowania środków prewencyjnych, najlepiej holistycznych lub co najmniej elementarnych, skupiających się na najbardziej newralgicznych punktach styku interesu firmy i pracownika.

BYOD z pewnością nie jest modelem, który znajdzie uznanie w każdej organizacji, wynikać to może z rodzaju prowadzonej działalności, wielkości przedsiębiorstwa czy zasobów, na których operują pracownicy. Koncepcja BYOD mimo swoich wad stanowi jednak wartościowy i rozwojowy model biznesowej kooperacji pracownika i firmy.

Literatura

1. Chmielewski J. (2017), *Czynnik ludzki a bezpieczeństwo informatyczne nowoczesnych przedsiębiorstw*, [w:] Jędrzejczyk W., Kobis P., Kucęba R. (red.), *Behawioralizm w teorii i praktyce zarządzania. Kreowanie kapitału ludzkiego, strukturalnego i społecznego organizacji*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa.

2. Griffin R.W. (2017), *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa.
3. http://ksiegowosc.infor.pl/podatki/pit/pit/dzialalnosc-gospodarcza/746007,Nieodplatne-swiadczenie-uslug-skutki-podatkowe.html (dostęp: 18.04.2018).
4. https://news.microsoft.com/pl-pl/2015/01/26/byod-po-polsku/ (dostęp: 17.04.2018).
5. https://securelist.com/threats/byod-glossary/ (dostęp: 15.03.2018).
6. https://sjp.pl/ryzyko (dostęp: 18.04.2018).
7. https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf (dostęp: 15.04.2018).
8. https://www.kaspersky.pl/o-nas/informacje-prasowe/2468/kaspersky-lab-zagrozenia-dotyczace-polityki-byod-sa-czesto-ignorowane-zwlaszcza-przez-male-firmy (dostęp: 15.04.2018).
9. https://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software (dostęp: 21.04.2018).
10. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod (dostęp: 18.04.2018).
11. Jaślan M. (2016), *BYOD nie wywołał w Polsce rewolucji*, „Reseller News", nr 7-8.
12. Jaślan M. (2017), *Ufać i kontrolować to zasada przy wdrażaniu BYOD*, „Reseller News", nr 5-6.
13. Jędrzejczyk W. (2015), *Współczesne technologie informacyjne v. systemy informacyjne przedsiębiorstw*, [w:] Kiełtyka L., Niedbał R. (red.), *Wybrane zastosowania technologii informacyjnych wspomagających zarządzanie w organizacjach*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.
14. Kiełtyka L. (2017), *Zarządzanie informacją i jej bezpieczeństwem w korporacji*, [w:] Kiełtyka L., Kobis P. (red.), *Wybrane zagadnienia zarządzania współczesnym przedsiębiorstwem*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.
15. Kobis P. (2017), *Zarządzanie w zakresie bezpieczeństwa informacji w małych i średnich przedsiębiorstwach*, „Przegląd Nauk Ekonomicznych", nr 27.
17. Portela F., Moreira da Vega A., Santos M. (2018), *Benefits of Bring Your Own Device in Healhcare*, [w:] Machado J., Abelha A. (eds.), *Next-Generation Mobile and Pervasive Healthcare Solutions*, IGI Global, Hershey.
18. Tarczyński W., Mojsiewicz M. (2001), *Zarządzanie ryzykiem. Podstawowe zagadnienia*, PWE, Warszawa.

BYOD AS A SIGNIFICANT ELEMENT OF CORPORATE OPERATIONAL RISK

Abstract: This article mainly relates to the problem of employing a BYOD (Bring You Own Device) trend in organizations, which is a corporate policy permitting employees to use their personally owned mobile devices to perform duties at work, including accessing company resources (https://securelist.com/…). The article presents the advantages and disadvantages of implementing this solution in entity structures. Furthermore, it also attempts to depict the dimension of BYOD implementation risk, in particular how this implementation refers to the level of operational risk incurred by a company. Moreover, it presents a threat map and the vectors of threat influence on the enterprise. Finally, the article indicates the main methods allowing to minimize danger resulting from employing this trend and it also answers the questions related to information safety in organizations which implemented a BYOD solution within their structures.

Keywords: BYOD, consumerization, operational risk, threats, security, staff