KRÓTKI PRZEWODNIK PO

B.Y.O.D

D-Link®

SPIS TREŚCI

WPROWADZANIE 3

KROK 1: OPRACOWAĆ PLAN 4

Przygotowanie wstępnego projektu polityki BYOD . . 4

Zgodność i regulacje prawne 4

Bezpieczeństwo i kontrola 5

Dostęp do aplikacji 5

Polityka bezpieczeństwa 6

Bezpieczeństwo aplikacji 6

Nowe aplikacje 6

Prywatność użytkowników 6

Koszt danych mobilnych 7

Zgodny 7

KROK 2: OMÓWIĆ PLAN 8

KROK 3: WYBRAĆ LAN 9

OPCJA 1: Oprogramowanie 9

OPCJA 2: Sprzęt 10

WNIOSKI 11

BIBLIOGRAFIA 12

WPROWADZENIE

Wdrożenie programu BYOD bez dobrego przygotowania i planu szybko może stać się przyczyną dużego zamieszania i obciążenia działu IT.

Zamiast ułatwić pracownikom dostęp do plików, źle wdrożona polityka BYOD może wygenerować coraz większą kolejkę zapytań do pomocy technicznej i powodować wzrost niezadowolenia wśród pracowników.

To tylko część powodów dla których zaledwie kilka lat temu prawie połowa firm zakazała praktyk związanych z programem BYOD.[1] TDo tego doszły rosnące obawy dotyczące naruszenia prawa, złośliwego oprogramowania, ransomware'u oraz hakowania.

Jednak od tamtego czasu wszystko się zmieniło. Obecnie blisko 60% firm wprowadziło politykę BYOD[2], która niesie ze sobą wiele korzyści.

Oto tylko niektóre z nich:

- Pracownicy w firmach, które wdrożyły programy BYOD, każdego dnia oszczędzają średnio 58 minut i są o 34% bardziej produktywni.[3]
- Programy BYOD mogą przynieść oszczędności do 350 dolarów na pracownika.[4]
- Urządzenia pracowników często są nowocześniejsze i mają większe możliwości niż urządzenia firmowe.
- Prawie dwa miliardy dolarów rocznie[6] – tyle można uzyskać dzięki wzrostowi produktywności przy korzystaniu z szybszych i wydajniejszych urządzeń

Właściwie wdrożony program BYOD przekłada się nie tylko oszczędność czasu i pieniędzy, ale jest czynnikiem poprawiającym bezpieczeństwo. Jednym z głównych powodów włamań i wycieku danych jest bowiem korzystanie z przestarzałych systemów oraz stosowanie niewystarczających zabezpieczeń.[5]

Nie oznacza to, że skuteczne okaże się proste dodanie zabezpieczeń do systemu BYOD. Trzeba pamiętać, że skala ochrony urządzeń BYOD to pochodna odpowiednich zabezpieczeń stosowanych w firmach. Trzeba też pamiętać, że smartfony to jedne z najczęściej atakowanych i podatnych na ataki urządzeń mobilnych. Zarazem to właśnie z nich pracownicy będą korzystać najczęściej.

Co należy zrobić, aby osiągnąć założony cel:

OPRACOWAĆ PLAN • **OMÓWIĆ PLAN** • **WYBRAĆ PLAN**

KROK 1 - OPRACOWAĆ PLAN

PRZYGOTOWANIE WSTĘPNEGO PROJEKTU POLITYKI BYOD

Politykę BYOD trzeba traktować zarówno jako element sieci lub też jako dodatek do niej. Wiele polityk i regulacji, które już obowiązują w firmie, będzie się odnosić także do prywatnych urządzeń mobilnych pracowników.

Przedmiotem regulacji jest cel, dla którego pracownicy korzystają z sieci firmowej, plików oraz treści do których mają dostęp, jak też informacji i danych, którymi mogą lub nie dzielić się z innymi.

W większości przypadków wprowadzenie polityki BYOD przekłada się na korzyści dla firmy. Pracownicy zyskają możliwość wykonywania pracy zdalnie i będą mieć dostęp do narzędzi zwiększających produktywność.

Niestety, BYOD stwarza więcej możliwości dla osób planujących kradzież lub włamanie do firmowych urządzeń. Dlatego pierwszym krokiem w opracowaniu polityki BYOD jest plan.

Oto zagadnienia, którym należy się przyjrzeć podczas przygotowania planu:

ZGODNOŚĆ I REGULACJE PRAWNE

Zanim pracownicy uzyskają dostęp do poufnych danych firmy, chociażby z ich ulubionej kawiarni, trzeba upewnić się, że zostali poinformowani o wszystkich konsekwencjach wynikających z regulacji prawnych.

Udostępnienie sieci firmowej urządzeniom mobilnym może zwiększyć liczbę lokalnych, regionalnych i narodowych regulacji, które znajdą zastosowanie w tej sytuacji, jak np. General Data Protection Regulation (GDPR), które w Unii Europejskiej weszło w życie w 2018 r. Ważne jest zrozumienie tych zapisów na tyle, by jasno zakomunikować ich szczegóły pracownikom.

Gdy to zostanie już zrobione, wówczas przyjdzie czas na opracowanie szczegółów działania na wypadek, gdyby któryś z pracowników kiedykolwiek je złamał lub doszło do ich naruszenia.

Przygotowanie takich planów niekoniecznie oznacza, że uda się powstrzymać każde potencjalne naruszenie polityki. Jednak zwiększa szansę na to, by utracony telefon nie był źródłem wycieku danych wartego wiele milionów.

BEZPIECZEŃSTWO I KONTROLA

Odkąd ustanowiono zasady, zawsze znalazł się ktoś, kto próbował je obejść.

Czy akceptujemy to, czy nie, dotyczy to także zatrudnionych pracowników. Aż 95 procent firm zgłosiło przynajmniej jedną próbę obejścia zabezpieczeń.[7] Obejmują one takie działania jak jailbreaking urządzeń w celu obejścia uprawnień roota w Androidzie, iOS oraz innych mobilnych systemach operacyjnych, jak też próby usunięcia firmowego oprogramowania zarządzającego z urządzenia.

Firma musi mieć przygotowane procedury na wypadek, gdyby doszło do któregoś z tych działań. Plan powinien obejmować działania wewnętrzne oraz działania dyscyplinarne.

To może być automatyczna kwarantanna dla urządzeń do czasu, gdy będą one spełniać wszystkie wymogi bezpieczeństwa, nałożenie kar dyscyplinarnych oraz inne działania. Pracownicy powinni zostać o nich poinformowani, zanim zaczną korzystać ze swoich prywatnych urządzeń.

W większości przypadków próby jailbreakingu lub usunięcia oprogramowania są podejmowane bez zamiaru wyrządzenia szkody. Jednak z pewnością sprawiają, że urządzenia są bardziej podatne na ataki. Celem ataków złośliwego oprogramowania są zazwyczaj przestarzałe i mniej bezpieczne urządzenia, aplikacje oraz słabe hasła. Pliki firmowe zawierają też poufne informacje o pracownikach.

Zasoby systemów HR to drugie najbardziej pożądane informacje tuż pod danych firmowych. Jeden profil lub folder z danymi osobistymi można sprzedać na czarnym rynku za około 50 dolarów.[8]

Tak więc zanim zezwoli się na korzystanie z prywatnych urządzeń w pracy, trzeba szczegółowo poinformować pracowników o kwestiach zgodności i zabezpieczeniach. A następnie przygotować plan na to, co nieuchronne.

DOSTĘP DO APLIKACJI

Jak już wspomniano, aplikacje są podatne na ataki, dlatego należy zdecydować, które z nich mogą być używane na urządzeniach pracowników i jak je monitorować. Korzystanie z niektórych może zależeć, od tego, co trzeba zrobić, aby zapewnić ich zgodność. Nie wszystkie aplikacje spełniają bowiem standardy bezpieczeństwa lub wymogi prawne.

Należy rozważyć tutaj kilka kwestii:

POLITYKA BEZPIECZEŃSTWA

Obostrzenia mogą umożliwiać korzystanie jedynie z zatwierdzonych przez firmę aplikacji. Takie podejście będzie stanowić problem dla pracowników ze starszymi urządzeniami, które nie będą obsługiwać nowych aplikacji. Jednak z drugiej strony, jeśli da się pracownikom możliwość wyboru aplikacji, z których chcą korzystać, może to być problem dla wydajnego działania sieci.

BEZPIECZEŃSTWO APLIKACJI

Z pewnością łatwiej nadzorować kwestie kompatybilności, bezpieczeństwa i zgodności, jeśli do użytku zostaną dopuszczone jedynie aplikacje zatwierdzone przez firmę. Z takim podejściem związane jest jednak ryzyko, co zrobią pracownicy.

W końcu o ile Facebook lub Twitter mogą jedynie rozpraszać i prowadzić do mniejszej produktywności, menedżer odpowiedzialny za media społecznościowe może potrzebować aplikacji kontrolującej posty i komentarze umieszczane na firmowych stronach.

NOWE APLIKACJE

Pracownicy zawsze będą szukać nowego oprogramowania i aplikacji, które pomogą im w wykonywaniu pracy. Czy należy dopuścić je do użytku?

Niektóre firmy decydują się na umieszczenie takich aplikacji na czarnej liście, inne wprost przeciwnie, dodają je do białej listy, gdy tylko się pojawią. Ostatecznie wszystko zależy od czasu, jaki dział IT może poświęcić na zarządzanie nimi.

Jeśli jednak zablokowanie aplikacji ogranicza sprawdzanie poczty elektronicznej, korzystanie z kalendarza, kontaktów lub dostęp do WiFi oraz VPN, być może warto zastanowić się, czy podjęta decyzja jest słuszna.

PRYWATNOŚĆ UŻYTKOWNIKÓW

Prywatność to zawsze ważny temat. Przy okazji doniesień prasowych o tym, jak firmy radzą sobie zarówno z publicznymi, jak i prywatnymi danymi, dyskusje nad prywatnością rozpoczynają się na nowo. Niekiedy zaniechanie zbierania jakichkolwiek danych o pracownikach to efekt obowiązującego prawa.

Zasadniczo nie powinno się gromadzić informacji o pracownikach chyba, że jest to absolutnie konieczne. Jeśli takie dane są gromadzone, powinno się wykluczyć informacje osobiste, prywatne zdjęcia, treści wysyłanych wiadomości, zapisy rozmów głosowych oraz historie połączeń, adresy e-mail, danych pochodzące z użytkowanych aplikacji, informacje o kontaktach, wydarzeniach z kalendarzy i lokalizacji urządzeń.

W przypadku, jeśli zbierane dane bezpośrednio dotyczą spraw firmowych, pracownicy powinni dokładnie wiedzieć czego dotyczą. Nie ma wątpliwości co do tego, że dane firmowe, pliki, aplikacje i inne zasoby muszą być chronione.

Kontenery mogą oddzielić dane osobiste od firmowych, a jednocześnie chronić prywatność i umożliwiać zdalne kasowanie danych, jeśli zajdzie taka potrzeba. Przykładowo taka możliwość przyda się w sytuacji, gdy pracownik zgubił swój telefon, a zainstalowana na nim aplikacja zawiera informacje z firmowej karty kredytowej.

Bez względu na to, czy dane będą zbierane czy nie, pracownicy muszą zostać o tym poinformowani. Jeśli firma zdecyduje się na gromadzenie danych, pracownicy muszą wiedzieć, jakiego typu są to dane, w jakim celu gromadzone i czy mogą je zobaczyć.

Warto wspomnieć, że zbieranie informacji może odstraszyć pracowników od rejestrowania swoich urządzeń mobilnych, ograniczając możliwość gromadzenia danych w ogóle.[10] Zdecydowanie radzimy zrezygnować ze zbierania danych, o ile nie ma ku temu ważnego powodu.

KOSZT DANYCH MOBILNYCH

Osoby pracujące w domu mogą być zależne od dostępności danych mobilnych. Rodzi się pytanie, kto w takiej sytuacji płaci rachunek?

Niektóre firmy pokrywają wszystkie koszty związane z użyciem danych mobilnych, inne wyznaczają limity. Bez względu na to, które rozwiązanie zostanie przyjęte, konieczne jest utworzenie polityki, która jasno określi, które koszty są pokrywane i w jaki sposób.

Część z tych zadań można zrealizować za pomocą oprogramowania BYOD (więcej o tym poniżej).

POZWOLENIE

Gdy szczegóły programu zostały już dopracowane, nadal trzeba przejść przez proces rejestracji.

W taki czy inny sposób konieczne jest uzyskanie zgody pracowników na zapisy warunków korzystania z urządzeń BYOD. Wiele firm robi to poprzez oprogramowanie zarządzające. Trzeba upewnić się, że pracownicy wyrazili zgodę na przestrzeganie zapisów polityki (elektronicznie lub na wydrukowanych kopiach), zanim będą mogli dołączyć do programu BYOD.

Rejestracja za pomocą oprogramowania daje więcej kontroli nad poziomem zabezpieczeń, którego muszą przestrzegać pracownicy, jeśli chcą korzystać z sieci firmowej.

KROK 2 - OMÓWIENIE PLANU

Bez względu na to, jak szczegółowy będzie plan i jak wiele scenariuszy uwzględni, zawsze znajdzie się coś, co umknęło uwadze.

To jest powód dla którego konieczne jest omówienie planu z pracownikami. Może to odbywać się na spotkaniach, w formie ankiety lub nawet próśb o sugestie i zmiany.

Każda informacja zwrotna jest ważna, ta pochodząca od CEO firmy, oraz od po pracowników zatrudnionych tymczasowo. To szansa na wyjaśnienie powodów wprowadzenia polityki BYOD.

Należy zebrać informacje o urządzeniach i aplikacjach, których potrzebują pracownicy i z których już korzystają. Bezwzględnie należy pozwolić na zadawanie pytań, pamiętając jednocześnie że na tym etapie nie ma głupich pytań.

Jeśli ktoś spyta „Czy to ma wpływ na ekspres do kawy?" trzeba założyć, że jest powód, dla którego takie pytanie zadano. Może pracownik używa aplikacji do kontroli ekspresu i ma obawy, że aplikacja przestanie działać?

Bez względu na to, czego dotyczy pytanie, ostatnią rzeczą, którą można zrobić jest wprowadzenie programu BYOD, który powstrzyma kogoś od korzystania z urządzenia lub aplikacji, która pomaga w wykonywaniu pracy.

Po zgromadzeniu informacji czas na następny krok, czyli ponowne przejrzenie planu. Może okazać się, że konieczne będzie wprowadzenie poprawek, by scalić wszystko tak, aby stało czytelne dla jak największej liczby pracowników.

Jeśli okaże się, że kolejne rewizje planu tworzą nowe ograniczenia zamiast możliwości, być może przygotowany program BYOD nie odpowiada wymogom firmy.

Wówczas trzeba opracować nowy plan.

KROK 3 - WYBÓR PLANU

Gdy etap wprowadzania poprawek dobiegł końca, firma powinna wreszcie mieć gotowy plan. Pozostało jego wdrożenie i tutaj można skorzystać z kilku opcji.

Jedną z nich jest modyfikacja obecnej infrastruktury sieciowej i ustanowienie polityki kontroli dostępu.

To stara szkoła, jednak jest skuteczna, jeśli dysponuje się odpowiednią wiedzą i czasem. Pozostałe dwie opcje wiążą się ze skorzystaniem z oprogramowania lub sprzętu.

Pokrótce omówimy argumenty za i przeciw.

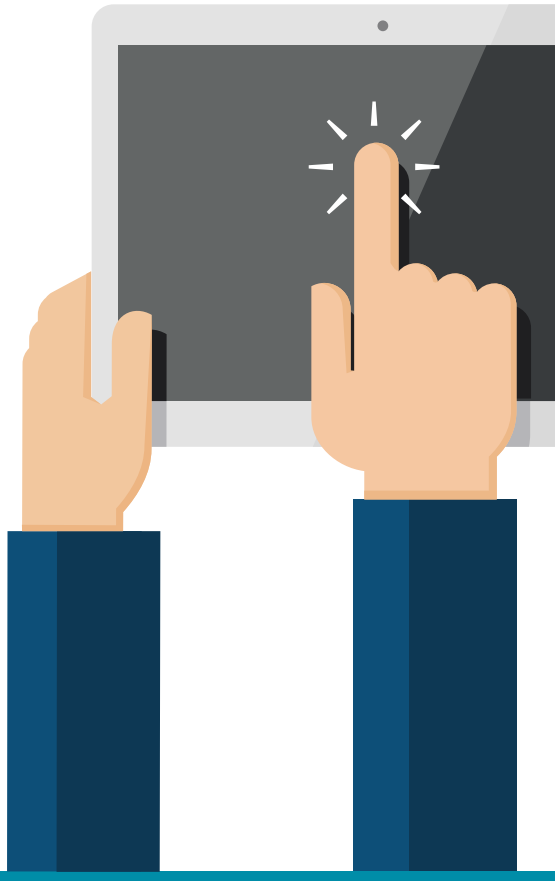
Jeśli opracowano plan i przedyskutowano jego założenia z pracownikami, trzeba zastanowić się, jak wszystkie poruszone kwestie wpłyną na funkcjonowanie firmy.

Najlepszą metodę wdrożenia wyznaczy budżet, pracownicy oraz infrastruktura.

OPCJA 1 - OPROGRAMOWANIE

Wiele firm decyduje się na zastosowanie w swoich programach BYOD oprogramowania Enterprise Mobility Management (EMM) lub Mobile Device Management (MDM). Większość narzędzi EMM obejmuje MDM lub Mobile Application Management (MAM). EMM pomaga w rejestrowaniu urządzeń, egzekwowaniu polityki, aktualizacji aplikacji oraz zarządzaniu dostępem.

Ma też przydatne funkcje takie jak alarmy użycia danych, kwarantannę urządzeń, oprogramowanie do zawierania umów z użytkownikami oraz uproszczone procedury rejestracyjne.



Narzędzie zarządzające wymaga, aby po rejestracji każdy z użytkowników pobrał i zainstalował oprogramowanie i dla każdego urządzenia zaakceptował umowę.

Ponieważ wszystkie ustawienia, polityki oraz aplikacje są zawarte w oprogramowaniu hostowanym na serwerze lub w chmurze, firma zyskuje więcej kontroli nad siecią, jej bezpieczeństwem oraz wydajnością.

Funkcjonalność EMM oraz MDM ułatwia dostosowanie ustawień do wybranych aplikacji lub grup aplikacji, co obejmuje także polityki regulujące czas i sposób, w jaki pracownicy mogą z nich korzystać.

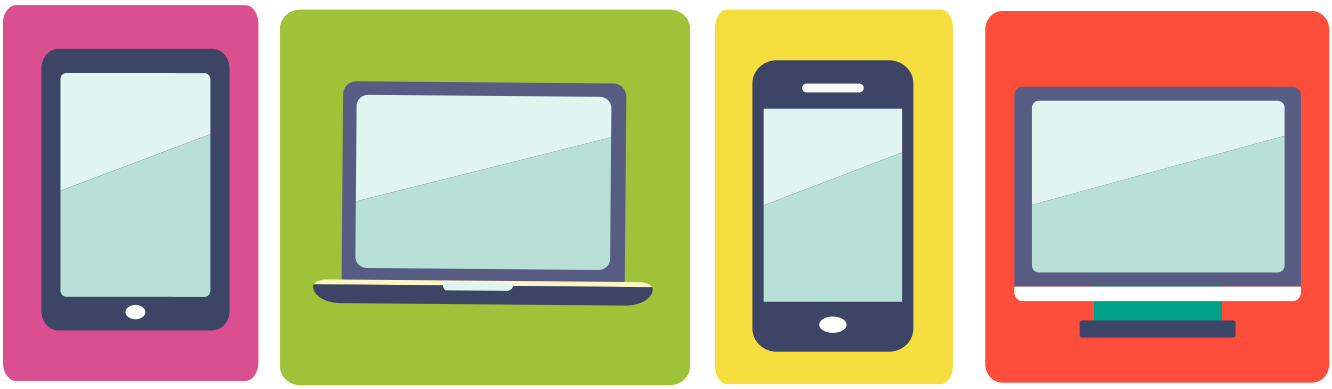
Za pomocą oprogramowania można także utworzyć osobne konta i dane uwierzytelniające do logowania dla wszystkich aplikacji

w sieci. Taka organizacja ułatwia bezpieczniejsze przechowywanie danych i zapewnia poufność wrażliwych informacji.

Większość opcji oprogramowania łatwo jest skalować. Zazwyczaj oferuje ono także kompletną listę zgodnych aplikacji i wbudowanych narzędzi do zarządzania, czego nie ma w rozwiązaniu opartym na sprzęcie. Pomimo oczywistych zalet, dla mniejszych organizacji korzystanie z oprogramowania może stanowić obciążenie budżetu.

Pakiet oprogramowania EMM powinien:
- ułatwić rejestrację pracowników
- ograniczyć lub wyeliminować zapytania do pomocy technicznej
- udostępniać hasło do resetowania opcji
- obejmować możliwość zlokalizowania utraconego urządzenia
- umożliwić zdalne wymazanie danych
- udostępniać każdemu pracownikowi podpisaną kopię polityki BYOD

Pakiet oprogramowania EMM powinien umożliwiać udostępnianie certyfikatów dla:
- Sieci Wi-Fi
- Poczty elektronicznej
- Kontaktów
- Kalendarzy
- Aplikacji
- Współdzielonych dysków
- Sieci VPN



OPCJA 2 - SPRZĘT

Rozwiązanie sprzętowe, choć nie ma wszystkich funkcji oferowanych przez oprogramowanie EMM, może okazać się atrakcyjniejsze cenowo.

Większość operacji odbywa się za pomocą sieciowego rozwiązania zarządzanego przez chmurę (CMN) na podstawie pełnionych funkcji, kontroli dostępu 802.1X, serwerów RADIUS, dwustopniowego uwierzytelnienia, SSID oraz innych ustawień sieciowych, które można dostosować do indywidualnych preferencji.

W tym modelu większość aplikacji będzie bądź hostowana na serwerze bądź zainstalowana na urządzeniach mobilnych pracowników. Jednak za pomocą CMN nie można wprowadzić ustawień właściwych dla aplikacji, co nie oznacza, że podejście CMN jest mniej bezpieczne, niż oprogramowanie.

Nadal można wymagać od pracowników zaakceptowania umowy określającej, z których aplikacji i funkcji mogą korzystać w sieci firmowej, a z których nie. Dostęp do sieci poprzez różne SSID oraz

hasła to kolejne zabezpieczenie urządzeń oraz danych. Warto pamiętać, że praktycznie trudno jest powstrzymać pracowników od dostępu do firmowych danych przez urządzenia prywatne.

W przypadku, gdy utracą swoje urządzenie, niewiele będzie można zrobić, by zdalnie wymazać z nich dane. (Chociaż można skorzystać z modelu hybrydowego – CMN razem z EMM.)

Chociaż CMN nie udostępnia wszystkich narzędzi EMM, to ma zalety, których nie ma w oprogramowaniu – szybkie wdrożenie, przewidywalną i przystępną cenowo skalowalność oraz usprawnienie wydajności sieciowej.

Ponieważ rozwiązanie CMN obejmuje przełączniki, punkty dostępowe oraz inne elementy, można traktować je jako aktualizację sieci. Jest to szczególnie ważne, jeśli wdrożenie EMM nie ma sensu, a podjęto decyzję o wprowadzeniu programu BYOD. To okazja do zaktualizowania sieci firmowej i pozbycia się przestarzałych przełączników oraz punktów dostępowych korzystających z mniej bezpiecznych standardów bezprzewodowych. W przypadku rozwiązań z szybkim lub zdalnym wdrożeniem łatwo można zwiększyć przepustowość, gdy będzie taka konieczność.

Wdrożone nowe przełączniki i punkty dostępowe automatycznie pobiorą i skopiują wszystkie ustawienia konfiguracyjne, które zostały wcześniej przygotowane. To realna oszczędność czasu, która może okazać się bardziej opłacalna niż EMM, jeśli trzeba dodać setki a nawet tysiące urządzeń mobilnych takich jak tablety.

WNIOSEK

Decyzja o wdrożeniu programu BYOD należy do firmy. W tym temacie jest wiele kwestii do rozstrzygnięcia, które obejmują zagadnienia bezpieczeństwa, zgodności i korzystania z aplikacji.

Jeśli w przypadku Twojej firmy taki czas już nadszedł, służymy pomocą, nawet jeśli teraz są to tylko pytania.

Chciałbyś dowiedzieć się więcej?
Skontaktuj się z nami:

eu.dlink.com/contact

BIBLIOGRAFIA

Więcej informacji:
12 Features That Make Cloud-Managed Networks Easy To Manage

Bibliografia

1. Hamblen M. The bring-your-own-device fad is fading [Internet]. Computerworld. Computerworld; 2015 [cited 2019Jun12]. Dostępne na:: https://www.computerworld.com/article/2948470/the-bring-your-own-device-fad-is-fading.html

2. Bullock L. The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future [Internet]. Forbes. Forbes Magazine; 2019 [cited 2019Jun12]. Dostępne na:: https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#61b002f01f30

3. Employees Say Smartphones Boost Productivity [Internet]. Samsung Business Insights. 2018 [cited 2019Jun12]. Dostępne na:: https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/

4. DMS Technology. 3 Big Risks of BYOD [Internet]. DMS Technology. DMS Technology /wp-content/uploads/2016/01/DMS_LogoBlack.png; 2017 [cited 2019Jun12]. Dostępne na:: https://www.dmstechnology.com/3-big-risks-of-byod/

5. Dacri B. Thousands of Organizations Run the Majority of their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach [Internet]. BitSight. [cited 2019Jun12]. Dostępne na:: https://www.bitsight.com/press-releases/thousands-organizations-run-majority-of-computers-on-outdated-operating-systems

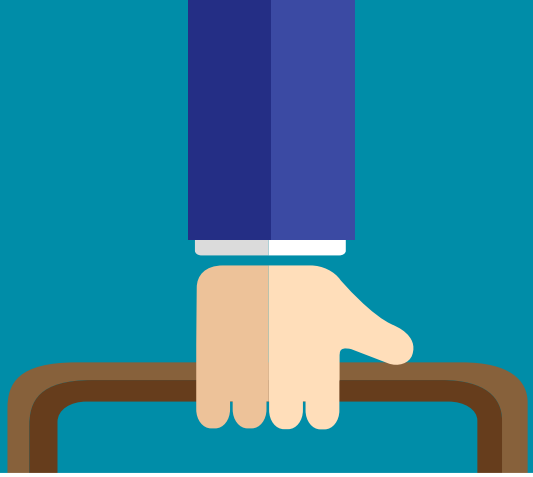
6. bizjournals.com. [cited 2019Jun12]. Dostępne na:: https://www.bizjournals.com/phoenix/news/2018/11/15/outdated-technology-costs-businesses-more-than-it.html

7. Bolden-Barrett V. Employees use personal devices for work without much oversight [Internet]. HR Dive. 2018 [cited 2019Jun12]. Dostępne na:: https://www.hrdive.com/news/employees-use-personal-devices-for-work-without-much-oversight/523913/

8. Bolden-Barrett V. HRIS, ATS technology is big target of cybertheft [Internet]. HR Dive. 2017 [cited 2019Jun12]. Dostępne na:: https://www.hrdive.com/news/hris-ats-technology-is-big-target-of-cybertheft/435599/

9. Ng A. Your smartphones are getting more valuable for hackers [Internet]. CNET. CNET; 2018 [cited 2019Jun12]. Dostępne na:: https://www.cnet.com/news/your-smartphones-are-getting-more-valuable-for-hackers/

10. IoT and BYOD Devices Bring Holiday Fear [Internet]. GetApp Lab. 2019 [cited 2019Jun12]. Dostępne na:: https://lab.getapp.com/iot-and-byod-devices/



D-Link®

KRÓTKI PRZEWODNIK PO B.Y.O.D