G DATA

Mobile Device Management

Nowoczesne modele pracy – BYOD i konsumeryzacja IT

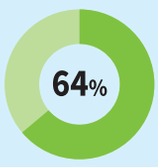
Nowoczesny biznes staje się coraz bardziej mobilny: od menedżerów przygotowujących umowy podczas lotów międzykontynentalnych, po pracowników sprawdzających pocztę w metrze. Utrzymanie takiego modelu pracy wymaga wprowadzenia urządzeń umożliwiających tworzenie wygodnego, cyfrowego środowiska pracy całkowicie niezależnego od miejsca przebywania pracownika.

Na myśl przychodzą automatycznie dwa pojęcia związane z obsługą urządzeń mobilnych w przedsiębiorstwach: konsumeryzacja oraz BYOD (Bring Your Own Device). Oba pojęcia stawiają użytkownika i jego potrzeby w centrum uwagi działów IT. Pracownik sam decyduje o wykorzystywanych aplikacjach oraz otrzymuje możliwość wykorzystywania prywatnego sprzętu do zadań służbowych. Zezwalając na BYOD, przedsiębiorstwa mogą znacznie zredukować koszty zakupu sprzętu. Haczyk: prywatne urządzenia nie są własnością przedsiębiorstw. Luki w zabezpieczeniach urządzeń mogą potencjalnie zagrozić sieci przedsiębiorstwa - z drugiej strony umożliwienie użytkownikom stosowania dowolnych aplikacji może znacząco wpłynąć na ich wydajność.

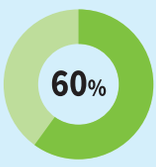
Podobne problemy mogą wystąpić w przypadku urządzeń służbowych: jeśli użytkownicy stosują na nich niezabezpieczone aplikacje do użytku prywatnego, może to wpływać na bezpieczeństwo oraz wydajność. Niezależnie od tego, czy urządzenie jest własnością pracownika, czy pracodawcy: jeśli zaginie lub zostanie skradzione, zagrożone mogą być dane przedsiębiorstwa. Niedbałość w kwestii planowania strategii zabezpieczeń może skutkować podejrzeniem, skopiowaniem lub usunięciem wrażliwych maili, zdjęć i dokumentów.

Utrata danych i malware to nie jedyne formy zagrożeń. Podczas przeglądania internetu spreparowane strony nakłaniają użytkowników do wprowadzania wrażliwych danych do niegroźnie wyglądających formularzy, w efekcie pozyskując poufne dane. Phishing oraz ataki drive-by--download zagrażają smartfonom i tabletom podobnie jak w przypadku komputerów osobistych.

> Kluczowe jest zapewnienie bezpieczeństwa mobilnego biura z zachowaniem wysokiego poziomu komfortu pracownika.



osób decyzyjnych czyta maile na urządzeniach mobilnych



zatrudnionych ma dostęp do firmowych danych spoza biura

Źródło: CyberEdge 2016 Cyberthreat Defense Report

nowych zagrożeń na system Android powstaje codziennie

Źródło: G DATA Software AG

urządzenia mobilne są stale postrzegane jako najsłabszy punkt infrastruktury przedsiębiorstw

Źródło: IBM

Maksymalne bezpieczeństwo – minimalny nakład pracy

Zarządzanie politykami bezpieczeństwa umożliwia administratorom czerpanie korzyści z nowoczesnych metod pracy bez wpływu na bezpieczeństwo. Dystrybucja oprogramowania zabezpieczającego urządzenia mobilne nigdy nie była prostsza. Zastosowanie wspólnego interfejsu do wszystkich zadań związanych z zarządzaniem urządzeniami mobilnymi podnosi wydajność pracy i jednocześnie redukuje koszty wdrożenia i zarządzania. Ilość urządzeń mobilnych wzrasta wraz z rozwojem przedsiębiorstwa - każde nowe urządzenie można łatwo wcielić do struktury zarządzania urządzeniami mobilnymi (MDM). Dystrybucja polityk i stosowanych aplikacji jest sterowana centralnie. Komunikacja z urządzeniami odbywa się poprzez internet, za pomocą poleceń push z chmury lub poprzez spreparowane polecenia SMS. W przypadku urządzeń z iOS stałe połączenie serwera zarządzającego nie jest wymagane: urządzenia stosują zdefiniowane polityki nawet w czasie gdy nie mają bezpośredniej łączności z serwerem.

Mobile Device Management zapewnia ochronę urządzeń przez cały czas, nawet po wyniesieniu urządzeń poza środowisko przedsiębiorstwa.

Co G DATA może zrobić dla Ciebie?

Mobile Device Management (MDM) to kwestia zaufania. Dostarczamy bezpieczne i sprawdzone rozwiązanie do zarządzania:

- **Informacje**: przejrzysty interfejs zarządzania umożliwia łatwe kontrolowanie wszystkich urządzeń w sieci przedsiębiorstwa
- **Dystrybucja**: administratorzy mogą łatwo wdrożyć oprogramowanie na urządzeniach mobilnych w sieci
- **Bezpieczeństwo**: moduł antykradzieżowy ułatwia odnalezienie zagubionych i skradzionych urządzeń. Zdalne usuwanie danych z urządzenia pomaga chronić wrażliwe dane firmowe
- **Restrykcje**: pracownicy mają dostęp tylko do niezbędnych aplikacji

Gdzie znaleźć G DATA MDM?

W zależności od potrzeb, możemy dopasować idealny sposób implementacji MDM:

- G DATA Mobile Internet Security oraz G DATA Action Center: hostowane rozwiązanie MDM w postaci G DATA ActionCenter to idealne rozwiązanie dla niewielkiej ilości urządzeń. Bez potrzeby stosowania dodatkowego sprzętu i dystrybucji oprogramowania administratorzy mogą zarejestrować swoje urządzenia mobilne i łatwo nimi zarządzać
- Wszystkie rozwiązania G DATA Business zawierają moduł Mobile Device Management. Umożliwia to całościowy przegląd wszelkich aspektów bezpieczeństwa sieci, łącznie z zabezpieczeniem urządzeń mobilnych
- G DATA Managed Endpoint Security: model G DATA w postaci usługi zarządzanej umożliwia wykorzystanie potencjału i infrastruktury Partnerów G DATA eliminując potrzebę inwestowania w sprzęt i obsługę
- G DATA Managed Endpoint Security: nasze produkty w połączeniu z usługą polskiej chmury obliczeniowej to dla partnerów G DATA proste i skalowalne rozwiązanie, zapewniające wysoką dostępność i elastyczność .

Korzyści z wprowadzenia BYOD:
- Polityka BYOD umożliwia wykonywanie obowiązków poza firmą
- W rezultacie stosowania BYOD, użytkownicy bardzo dobrze znają urządzenia, na których pracują
- Przedsiębiorstwa mogą zredukować koszty inwestycyjne dotyczące sprzętu

Zagrożenia dla urządzeń mobilnych:
- Cyberataki na urządzenia mobilne (malware, phishing)
- Utrata urządzenia może spowodować utratę danych
- Spadek wydajności (nadużywanie aplikacji niezwiązanych z obowiązkami)

Co daje MDM?
- Kontrolowanie urządzeń mobilnych
- Płynna dystrybucja oprogramowania
- Zintegrowane zarządzanie
- Antimalware/Antiphishing
- Moduł antykradzieżowy
- Lokalizowanie przez GPS
- Blokowanie urządzeń/usuwanie prywatnych danych
- Zarządzanie wydajnością
- Zarządzanie politykami bezpieczeństwa
- Czarne/białe listy aplikacji

Administratorzy mogą wybrać rozwiązanie MDM zintegrowane ze stosowanymi strukturami zarządzania aby zminimalizować nakład pracy. Idealnym rozwiązaniem jest zastosowanie wspólnego interfejsu do zarządzania i raportowania wszystkich typów urządzeń w sieci w celu zapewnienia spójnego przepływu danych i modelu konfiguracji.

Nowe urządzenia dopuszczone do użytkowania powinny zostać zaopatrzone w odpowiednie zabezpieczenia jeszcze przed przekazaniem ich użytkownikom. Urządzenia BYOD powinny mieć zablokowany dostęp do sieci i zasobów przedsiębiorstwa przed wcieleniem ich do struktury MDM. Wyjątkiem może być dostęp do wydzielonej sieci dla gości, dla urządzeń niespełniających wymagań bezpieczeństwa zdefiniowanych dla przedsiębiorstwa.

Więcej informacji: www.gdata.pl/go/business
Wymagania systemowe: www.gdata.pl/go/wymagania

G DATA MADE IN GERMANY