Praca zdalna z Apple. Jak zadbać o bezpieczeństwo danych?

W czasach, kiedy możliwość pracy zdalnej stała się nie tylko przywilejem, ale także warunkiem do sprawnego funkcjonowania wielu przedsiębiorstw, warto poszukać odpowiednich rozwiązań. Przeorganizowanie pracy całych zespołów wiąże się z wyzwaniami, a do nowych warunków dostosować się muszą zarówno pracownicy jak i pracodawcy. W tej sytuacji potrzebne są narzędzia, które zapewnią nie tylko komfortowe warunki pracy poza biurem, ale także sprawią, że praca będzie wydajna i przede wszystkim bezpieczna.
W tej roli doskonale sprawdzą się urządzenia od Apple.

Bezpieczeństwo to podstawa

Podczas pracy poza biurem, nasze dane firmowe, mogą być narażone na duże niebezpieczeństwo. Utrata cennych informacji może przedsiębiorstwo wiele kosztować, dlatego warto być ostrożnym, a do kwestii bezpieczeństwa przywiązać szczególną uwagę.

MacOS zawiera wbudowane rozwiązania techniczne, które pomagają w prostym zarządzaniu i ochronie przed złośliwym oprogramowaniem. Zadba również o instalowanie wyłącznie zaufanych aplikacji. Dodatkowo każdy Mac wyposażony jest we wbudowany mechanizm szyfrujący, FileVault, który zabezpiecza wszystkie dane przechowywane w pamięci masowej komputera. Na straży bezpieczeństwa stoi także szereg innych, wbudowanych systemów, które zapewnią bezpieczeństwo Twojej organizacji.

Niestety, pomimo szeregu wbudowanych systemów, okazuje się, że zagrożeniem może być sam użytkownik. Dlatego warto pamiętać, że wiele zagrożeń dla bezpieczeństwa można zmniejszyć, wdrażając odpowiednie rozwiązania w sieci.

Jak bezpiecznie zarządzać urządzeniami Apple podczas pracy zdalnej?

Przedstawiamy kilka cennych porad.

1. Upewnij się, że wykorzystywana technologia jest odpowiednia do utrzymania poziomu bezpieczeństwa.

Przenosząc wszystkie operacje poza korporacyjną zaporę sieciową, ważne jest, aby urządzenia i systemy były nie tylko dostępne dla pracowników, ale też odpowiednio chronione. Apple kładzie ogromny nacisk na szyfrowanie i ochronę danych w najnowszych wersjach wszystkich systemów operacyjnych, dając tym samym najlepszą z możliwych ochronę – zarówno użytkownikom jak i całym organizacjom.

Zasada ochrony prywatności użytkowników ma także zastosowanie w kontach iCloud, co uzupełnia obraz bezpieczeństwa w ekosystemie Apple.

Aby jeszcze bardziej zwiększyć bezpieczeństwo swojego środowiska, możesz wykorzystać takie rozwiązanie, jak jamf protect. Rozwiązanie to może rozszerzyć możliwości bezpieczeństwa poprzez raportowanie i analizę zagrożeń bezpośrednio występujących na urządzeniu. Gwarantuje to, że gdziekolwiek pracują Twoi pracownicy, zawsze możesz szybko zareagować, aby Twoje dane firmowe pozostały bezpieczne.

2. Skontroluj zasady cyberbezpieczeństwa obowiązujące w Twojej organizacji.

Celem polityki bezpieczeństwa jest wskazanie środków bezpieczeństwa i procedur bezpiecznego przetwarzania informacji.
Określa ona:

- Aktywa, które należy chronić
- Zagrożenia dla tych aktywów
- Zasady ochrony tych aktywów i Twojej firmy

Polityka bezpieczeństwa nie zakłóca produktywności pracowników i nie ogranicza dostępu do aplikacji i systemów niezbędnych do wykonywania służbowych obowiązków. Dzięki temu jest w stanie zaspokoić podstawowe potrzeby związane z pracą zdalną.

Należy zapewnić równowagę między ograniczeniami wprowadzanymi dla bezpieczeństwa danych firmowych a tym, do czego dostęp mają pracownicy. W ten sposób pozycja firmy pozostaje silna, bez narażania wydajności poszczególnych użytkowników.

Kluczowym krokiem do ustanowienia skutecznej polityki cyberbezpieczeństwa jest udokumentowanie i dystrybucja warunków użytkowania i wykorzystywania zasobów firmowych przez pracowników. Bez względu na to, jak silna jest ochrona, użytkownicy mogą narażać firmę przez nieodpowiednie zachowania, np. na niebezpieczeństwo phishingu. Do takich działań należy, m.in. udostępnianie poufnych danych w mediach społecznościowych czy przekazywanie danych dostępowych nieupoważnionym osobom.

3. Utrzymuj silne i zróżnicowane hasła lub użyj Menedżera haseł

Zapewnienie silnych i zróżnicowanych haseł jest kluczowym wymaganiem biznesowym dla zapewnienia bezpieczeństwa przedsiębiorstwa.
Zdarza się, że podczas pracy zdalnej – przebywając poza siecią organizacji, pracownicy mają większe trudności z dostępem do swoich kont. Szczególnie uciążliwe może okazać się to dla supportu, który będzie mocno obciążony napływającymi prośbami o resetowanie haseł. Pomocne w tej sytuacji będzie korzystanie z menedżera haseł. Dzięki takiemu rozwiązaniu, użytkownik będzie miał dostęp do różnych systemów logując się jedynie do menedżera haseł. Konieczność zapamiętania tylko jednych danych dostępowych sprawi, że liczba zgłoszeń o występujących problemach z logowaniem będzie znacznie mniejsza.

W INNERGO Systems rozumiemy, że zarządzanie tożsamością i dostępem oraz bezpieczeństwo informacji to kluczowe funkcje w nowoczesnych organizacjach. Opierając się na wieloletnim doświadczeniu w budowaniu strategii mobilności przedsiębiorstwa, wspieramy w wyborze i wdrożeniu najlepszych rozwiązań.