KURS

Cyberbezpieczne środowisko w szkole

ATOM 9

Jak bezpiecznie pracować w chmurze Microsoft?

PROWADZĄCY

Artur Rudnicki
Microsoft Innovative Educator Expert

Bezpieczeństwo w chmurze jest kluczowym elementem dla każdej organizacji korzystającej z usług takich jak Office 365. W dobie cyfryzacji, ochrona danych i zapewnienie ich integralności staje się priorytetem. Office 365 oferuje szereg narzędzi i funkcji, które pomagają w zabezpieczeniu danych, takich jak zaawansowane mechanizmy uwierzytelniania, szyfrowanie danych oraz monitorowanie aktywności użytkowników.

Oto podstawowe zasady bezpiecznej pracy w chmurze:

1. **Używaj silnych haseł i uwierzytelniania wieloskładnikowego (MFA)**
   - Hasła powinny być złożone i unikalne dla każdego konta.
   - Uwierzytelnianie wieloskładnikowe (MFA) dodaje dodatkowy poziom ochrony, nawet jeśli hasło zostanie skompromitowane.
2. **Regularne aktualizacje i łatki bezpieczeństwa**
   - Regularnie aktualizuj oprogramowanie i aplikacje w chmurze, aby zapobiegać wykorzystaniu luk w zabezpieczeniach.
3. **Szyfruj dane**
   - Dane powinny być szyfrowane zarówno podczas przesyłania, jak i w stanie spoczynku (przechowywania).
   - Szyfrowanie pomaga chronić informacje przed dostępem nieuprawnionych osób, nawet jeśli dojdzie do ich przechwycenia.
4. **Korzystaj z autoryzowanego dostępu i nadawaj minimalne uprawnienia**
   - Ograniczaj dostęp do zasobów w chmurze, przydzielając użytkownikom minimalne uprawnienia, które są potrzebne do wykonywania ich zadań.
   - Regularnie przeglądaj listę użytkowników i ich poziom dostępu.

5. **Twórz regularne kopie zapasowe danych**
    - Zapewnij regularne tworzenie kopii zapasowych danych przechowywanych w chmurze, aby móc odzyskać je w razie awarii lub ataku.
6. **Monitoruj aktywność i wykrywaj zagrożenia**
    - Korzystaj z narzędzi do monitorowania i analizy aktywności, aby wykrywać podejrzane zachowania lub potencjalne zagrożenia.
    - Systemy detekcji mogą szybko zidentyfikować nietypowe logowania lub transfery danych.
7. **Edukacja i świadomość użytkowników**
    - Regularnie szkol pracowników na temat bezpiecznego korzystania z chmury oraz rozpoznawania zagrożeń, takich jak phishing czy inne techniki socjotechniczne.
8. **Zgodność z przepisami i regulacjami (np. GDPR)**
    - Upewnij się, że przetwarzanie i przechowywanie danych jest zgodne z obowiązującymi przepisami, w tym z RODO (GDPR), jeśli przetwarzasz dane osobowe obywateli UE.
    - Dokumentuj, jak przechowujesz i przetwarzasz dane, oraz stosuj politykę prywatności, aby sprostać wymaganiom regulacyjnym.
9. **Zabezpieczenia fizyczne i logiczne**
    - Jeśli korzystasz z prywatnych serwerów w chmurze, zadbaj również o fizyczne zabezpieczenia, np. dostęp do serwerowni.
    - Stosuj dodatkowe zabezpieczenia logiczne, takie jak firewalle i systemy wykrywania włamań.

Dwa słowa o silnych hasłach:

1. **Długość hasła**
    - Im dłuższe hasło, tym trudniej je złamać. Hasło powinno mieć co najmniej 12-16 znaków, a im dłuższe, tym lepiej.
2. **Różnorodność znaków**
    - Silne hasło powinno zawierać kombinację liter małych i wielkich, cyfr oraz znaków specjalnych (np. !, #, $, %).
    - Zróżnicowanie znaków zwiększa złożoność hasła i utrudnia atak słownikowy lub metodę brute force.
3. **Unikanie słów i sekwencji przewidywalnych**
    - Nie stosuj popularnych słów, zwrotów, czy fraz związanych z Twoimi danymi osobowymi (np. imię, nazwisko, data urodzenia).
    - Unikaj sekwencji przewidywalnych, takich jak „1234”, „qwerty” czy „password”.
4. **Hasła unikalne dla każdego konta**
    - Każde konto powinno mieć inne, unikalne hasło. Dzięki temu, jeśli jedno hasło zostanie skompromitowane, inne konta nadal pozostaną bezpieczne.
5. **Użycie menedżera haseł**
    - Menedżery haseł mogą pomóc w generowaniu i przechowywaniu silnych, unikalnych haseł dla każdego konta.
    - Menedżery haseł przechowują hasła w zaszyfrowanej bazie danych, umożliwiając szybki i bezpieczny dostęp.

6. **Regularna zmiana haseł**
    - W niektórych przypadkach zalecane jest regularne zmienianie haseł, szczególnie jeśli istnieje podejrzenie naruszenia bezpieczeństwa.
    - Pamiętaj jednak, że częsta zmiana hasła ma sens, gdy rzeczywiście wiąże się ze wzrostem jego złożoności, a nie tylko minimalnymi zmianami (np. dodanie jednej cyfry na końcu).
7. **Unikaj powtarzania fragmentów lub sekwencji klawiatury**
    - Powtarzające się znaki, sekwencje jak „asdfgh" czy „1111" obniżają bezpieczeństwo hasła.
8. **Uwierzytelnianie wieloskładnikowe (MFA)**
    - Nawet najsilniejsze hasło może zostać złamane, dlatego zaleca się stosowanie uwierzytelniania wieloskładnikowego (MFA), np. za pomocą aplikacji autoryzacyjnych, kluczy sprzętowych lub kodów SMS.

Przykład silnego hasła

Zamiast tworzyć hasło na zasadzie „Jan1234!", spróbuj zbudować frazę lub zdanie z wieloma elementami, np. „7KoronSierpnia!Przypadek19$", które łączy różne rodzaje znaków oraz cyfry w naturalny sposób.

Przegląd funkcji bezpieczeństwa dostępnych w Office 365.

1. **Ochrona przed zagrożeniami**
    - **Microsoft Defender for Office 365:** Chroni przed zaawansowanymi atakami, takimi jak phishing, złośliwe oprogramowanie czy spam. Oferuje funkcje takie jak bezpieczne linki i załączniki, które skanują i neutralizują potencjalne zagrożenia w czasie rzeczywistym.
2. **Uwierzytelnianie wieloskładnikowe (MFA)**
    - Dodaje dodatkową warstwę zabezpieczeń poprzez wymaganie więcej niż jednego sposobu weryfikacji tożsamości użytkownika podczas logowania. Pomaga to chronić konta nawet w przypadku ujawnienia hasła.
3. **Szyfrowanie danych**
    - **Szyfrowanie wiadomości e-mail:** Zapewnia, że tylko upoważnieni odbiorcy mogą odczytać treść wiadomości. Chroni przed nieautoryzowanym dostępem podczas przesyłania danych.
4. **Ochrona przed utratą danych (DLP)**
    - Monitoruje i chroni poufne informacje przed przypadkowym lub celowym wyciekiem. Umożliwia definiowanie zasad, które zapobiegają udostępnianiu wrażliwych danych nieuprawnionym osobom.
5. **Bezpieczne linki i załączniki**
    - **Safe Links:** Skanuje i weryfikuje linki w wiadomościach e-mail oraz dokumentach, neutralizując złośliwe adresy URL.
    - **Safe Attachments:** Analizuje załączniki w izolowanym środowisku przed ich dostarczeniem do odbiorcy, identyfikując potencjalne zagrożenia.

6. **Monitorowanie i raportowanie**
    - Zapewnia narzędzia do monitorowania aktywności użytkowników oraz generowania raportów dotyczących bezpieczeństwa, co umożliwia szybkie wykrywanie i reagowanie na potencjalne zagrożenia.
7. **Zarządzanie tożsamościami i dostępem**
    - **Usługa tożsamości Microsoft Entra:** Umożliwia zarządzanie tożsamościami użytkowników, kontrolę dostępu oraz implementację polityk bezpieczeństwa w całej organizacji.
8. **Bezpieczne współdzielenie plików**
    - Funkcje w OneDrive i SharePoint pozwalają na bezpieczne udostępnianie plików z kontrolą dostępu oraz możliwością ustawienia dat wygaśnięcia linków czy haseł zabezpieczających.