

Mały nośnik – duże ryzyko. Jak bezpiecznie korzystać z pamięci przenośnych i pendrive'ów

Podczas konferencji branżowej przedstawiciel jednej z firm otrzymał w materiałach powitalnych pendrive z prezentacjami sponsorów i katalogiem wydarzenia. Po powrocie do biura, chcąc pokazać współpracownikom ciekawą ofertę konkurencji, włożył nośnik do swojego służbowego laptopa. Komputer na chwilę się zawiesił, a potem wszystko wróciło do normy. Pracownik nie zwrócił na to większej uwagi.

Następnego dnia dział IT zauważył, że kilka komputerów w firmowej sieci zaczęło nietypowo obciążać łącze internetowe i wysyłać dane do nieznanych adresów IP. Szybko ustalono, że komputer przedstawiciela handlowego został zainfekowany złośliwym oprogramowaniem typu spyware, które automatycznie rozprzestrzeniło się w lokalnej sieci firmowej.

Śledztwo wykazało, że pendrive rozdawany na konferencji zawierał ukryty skrypt, który wykorzystywał lukę w autoodtworzeniu. Chociaż sam nośnik wyglądał jak zwykły gadżet reklamowy, okazał się wektorem ataku. Incydent wymagał odcięcia części komputerów od sieci, reinstalacji systemów i przeprowadzenia audytu. Firma przez trzy dni miała ograniczony dostęp do systemu CRM i poniosła realne straty operacyjne.

Wnioski były bolesne, ale jednoznaczne: żadnych pendrive'ów z niepewnego źródła i blokada automatycznego uruchamiania nośników USB we wszystkich komputerach. Od tej pory każdy nowy nośnik (np. pendrive czy dysk zewnętrzny) musi być zatwierdzony i przeskanowany przez dział IT, zanim zostanie użyty w jakimkolwiek urządzeniu firmowym.

Ryzyka i konsekwencje użycia nośników zewnętrznych

W dobie mobilności i pracy zdalnej pendrive'y pozostają jednym z najpopularniejszych sposobów przenoszenia danych. Ich wygoda, pojemność i niska cena sprawiają, że często wykorzystywane są w codziennej pracy – do przekazywania plików, kopiowania dokumentów, tworzenia szybkich backupów. Niestety, wraz z ich zaletami idą też konkretne zagrożenia, które w kontekście bezpieczeństwa danych mogą mieć poważne konsekwencje. W środowisku firmowym, gdzie informacje mają często charakter poufny lub podlegają przepisom prawnym, takim jak RODO, niekontrolowane użycie pamięci przenośnych może prowadzić do incydentów skutkujących np. wyciekiem danych, stratą wizerunkową lub odpowiedzialnością finansową.

Co może pójść nie tak?

- Pendrive zostaje zgubiony lub skradziony – dane trafiają w niepowołane ręce.
- Nośnik podłączony do komputera infekuje go złośliwym oprogramowaniem.

- Firmowe dane są bez nadzoru kopiowane na nośniki zewnętrzne i wynoszone z biura.

Zgubiony pendrive to scenariusz, który zdarza się częściej, niż mogłoby się wydawać. Wystarczy chwila nieuwagi – pośpiech na lotnisku, zapomniana torba w pociągu, pendrive pozostawiony w komputerze konferencyjnym. Jeśli dane na takim nośniku nie są odpowiednio zabezpieczone (np. zaszyfrowane), dostęp do ich zawartości jest niemal natychmiastowy. Przestępcy nie muszą włamać się do komputera czy sieci firmowej – wystarczy podłączyć urządzenie do portu USB, by uzyskać dostęp do potencjalnie wrażliwych informacji: danych klientów, faktur, umów czy nawet haseł.

Nie mniej groźny jest odwrotny scenariusz: to nie dane z pendrive'a zostają wykradzione, ale to właśnie pendrive staje się narzędziem ataku. Zainfekowane urządzenia USB są powszechnie wykorzystywane w atakach z użyciem złośliwego oprogramowania (malware) i oprogramowania wymuszającego okup (ransomware). W wielu przypadkach, by złośliwe oprogramowanie zaczęło działać – często bez wiedzy użytkownika - wystarczy włożenie nośnika do portu USB komputera. Dzieje się tak, gdy firma nie wyłączy funkcji autoodtwarzania lub nie stosuje ochrony antywirusowej. Co więcej, ataki tego typu bywają bardzo ukierunkowane – np. gdy napastnik celowo zostawia zainfekowany pendrive w siedzibie firmy, licząc, że ktoś z pracowników podłączy go z ciekawości.

Bezpieczne zasady korzystania z pamięci przenośnych

Skuteczna ochrona przed tymi zagrożeniami nie wymaga skomplikowanej technologii albo kosztownych rozwiązań technologicznych – wymaga natomiast konsekwentnego działania i świadomości zagrożeń. Przede wszystkim, każda organizacja – niezależnie od wielkości – powinna posiadać jasno sformułowaną **politykę bezpieczeństwa, która uwzględni korzystanie z pamięci przenośnych**. Dokument ten powinien określać, kto i w jakim zakresie może korzystać z tego typu urządzeń, jakie wymagania muszą one spełniać (np. szyfrowanie, rejestracja w firmowym systemie), oraz jakie działania będą podejmowane w przypadku incydentu.

Kluczowym elementem ochrony danych przechowywanych na pendrive'ach, dyskach zewnętrznych czy kartach pamięci jest ich **szyfrowanie**. Współczesne systemy operacyjne oferują proste w użyciu narzędzia, które pozwalają szybko zabezpieczyć nośnik hasłem lub certyfikatem. Dzięki temu nawet jeśli urządzenie trafi w niepowołane ręce, dostęp do zapisanych danych pozostaje praktycznie niemożliwy. Alternatywą są nośniki z wbudowanym szyfrowaniem sprzętowym, np. pendrive'y wymagające wpisania PIN-u.

Szyfrowanie odgrywa kluczową rolę nie tylko w ochronie samych nośników, lecz także w zapewnieniu zgodności z przepisami oraz utrzymaniu bezpieczeństwa informacji w organizacji. Ma ono szerokie zastosowanie:

- Ochrona danych osobowych – szyfrowanie zabezpiecza dane przed nieautoryzowanym dostępem, co jest kluczowe w kontekście wymagań RODO.

- Bezpieczeństwo informacji poufnych – firmy szyfrują dokumenty i pliki, aby zapobiec ich przejęciu przez konkurencję lub osoby trzecie.
- Minimalizacja skutków zgubienia lub kradzieży nośnika – odpowiednio zaszyfrowany pendrive staje się bezużyteczny dla osoby, która wejdzie w jego posiadanie bez hasła lub klucza.

W praktyce szyfrowanie może odbywać się na różnych poziomach.

- Szyfrowanie pełnego dysku. Chroni wszystkie dane na nośniku i zapewnia najwyższy poziom bezpieczeństwa.
- Szyfrowanie plików. Pozwala zabezpieczać wybrane pliki, oferując większą elastyczność, lecz pozostawiając pozostałe dane potencjalnie niechronione.
- Szyfrowanie transportu. Zapewnia bezpieczne przesyłanie danych pomiędzy urządzeniami a nośnikami.

Dobór właściwej metody szyfrowania powinien zależeć od rodzaju informacji i ich wrażliwości. Niezależnie jednak od tego, czy stosowane jest szyfrowanie pełnego nośnika, plików, czy rozwiązań sprzętowych, **kluczowe jest właściwe zarządzanie kluczami szyfrującymi**: ich bezpieczne przechowywanie, ograniczenie dostępu oraz regularna zmiana.

Drugą warstwą ochrony jest **kontrola portów USB**. System IT w firmie powinien umożliwiać blokowanie nieautoryzowanych urządzeń oraz identyfikację, kto i kiedy podłączył konkretny pendrive. W małych firmach wystarczy wdrożyć prosty rejestr wydawania nośników i ustalić zasadę, że tylko oznakowane, firmowe pendrive'y mogą być wykorzystywane do pracy. Ważne jest również regularne **skanowanie** tych urządzeń za pomocą programów antywirusowych posiadających aktualną bazę zagrożeń.

Blokowanie portów USB to prosta, ale bardzo skuteczna metoda ograniczania ryzyka. Dzięki temu nieautoryzowane urządzenia, np. nieznane pendrive'y, nie mogą być podłączane bez zgody administratora. Warto wprowadzić wyjątki dla konkretnych użytkowników lub stanowisk pracy, gdzie dostęp do USB jest rzeczywiście niezbędny.

Alternatywne rozwiązania – chmura i VPN

Praca z plikami w chmurze pozwala na bieżący dostęp do danych z dowolnego miejsca, bez ryzyka fizycznej utraty nośnika. VPN z kolei zapewnia bezpieczne połączenie z zasobami firmowymi i ogranicza potrzebę przenoszenia plików między urządzeniami. Oba rozwiązania pozwalają również centralnie zarządzać dostęпами i natychmiast reagować na incydenty bezpieczeństwa.

Pendrive nie musi być zagrożeniem. Może być bezpiecznym narzędziem pracy – ale tylko wtedy, gdy jego użycie odbywa się w sposób świadomy i kontrolowany. W przeciwnym razie, jedno niepozorne urządzenie może narazić całą firmę na poważne konsekwencje.

Najważniejsze zasady:

- Zawsze szyfruj dane na nośniku – nawet jeśli pendrive zostanie zgubiony, nikt nie odczyta jego zawartości.
- Zablokuj w komputerze możliwość korzystania z nieautoryzowanych urządzeń USB. Umożliwaj podłączanie tylko firmowych, zatwierdzonych pendrive'ów.
- Nie kopiuj danych bez potrzeby. Stosuj zasadę minimalizmu – nie przenoś danych, jeśli możesz pracować z nimi zdalnie przez VPN lub w chmurze.
- Wyłącz autoodtworzenie portów USB, by nie uruchomić złośliwego pliku.
- Skanuj pamięci przenośne programem antywirusowym.
- Oznaczaj i rejestruj firmowe pendrive'y.
- Edukuj pracowników na temat zasad korzystania z nośników.
- Traktuj zgubiony pendrive jako incydent bezpieczeństwa.

Checklista – bezpieczeństwo urządzeń przenośnych w firmie – pytania kontrolne

- Czy wszystkie pendrive'y są szyfrowane?
- Czy system blokuje nieautoryzowane urządzenia USB?
- Czy istnieje polityka bezpieczeństwa uwzględniająca korzystanie z pamięci przenośnych?
- Czy pendrive'y są skanowane programem antywirusowym?
- Czy firma prowadzi rejestr wydanych nośników?
- Czy kopiowanie danych na nośniki zewnętrzne odbywa się wyłącznie za zgodą pracodawcy i zgodnie z obowiązującymi procedurami?
- Czy dane na nośnikach są usuwane po zakończeniu pracy?
- Czy każdy incydent (zgubienie lub kradzież) jest niezwłocznie zgłaszany?
- Czy pracownicy są cyklicznie szkoleni w zakresie bezpiecznego korzystania z nośników?