Zabezpieczenia pamięci przenośnej według irlandzkiego organu nadzorczego

Co słychać na zielonej wyspie?

Jak dobrze wiemy, jednym z głównych obowiązków administratora danych wynikających z ogólnego rozporządzenia o ochronie danych (RODO) jest zapewnienie odpowiednich środków bezpieczeństwa danych osobowych. Te środki powinny chronić przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem (posługiwaniem się) danymi osobowymi, w tym przed kradzieżą, zniszczeniem, uszkodzeniem lub ich ujawnieniem. Skąd administrator danych osobowych ma wiedzieć jakie środki bezpieczeństwa są odpowiednie? Dokonując analizy ryzyka, zatrudniając specjalistów lub... samodzielnie czytając wytyczne organów. Należy również pamiętać o audycie (monitorowaniu) zastosowanych środków, ponieważ z czasem mogą się dezaktualizować. W tym wpisie skupimy wzrok na ostatnim przypadku, a dokładnie na przejrzeniu wytycznych irlandzkiego organu ochrony danych osobowych (1).

Pamięci przenośne – jak żyć?

Jeżeli w swojej firmie administrator danych nie zablokował portów USB, może dochodzić do zgrywania danych osobowych na masowe pamięci przenośne:

- pendrive,
- zewnętrzne dyski twarde,
- karty micro-SD,

bądź na wewnętrzne pamięci przenośne różnych urządzeń:

- smartfonów,
- tabletów.

Powyższe urządzenia z pamięciami przenośnymi należy zabezpieczyć analizując kwestie m. In.:

- przenoszenia urządzeń, a więc możliwość ich kradzieży lub zgubienia,
- wgrania złośliwego oprogramowania po podłączeniu do urządzenia służbowego,
- nieuprawnionego dostępu do plików przez osoby postronne.

Czy wewnętrzne firmowe procedury będą pomocne? Odpowiedź wydaje się oczywista – nie. Dokumentacja pozwala jedynie uporządkować środki, które powinny być stosowane w danym przypadku. Natomiast te środki bezpieczeństwa należy jeszcze zastosować i je sprawdzić. O jakich środkach bezpieczeństwa mowa? Z odpowiedzą przychodzi właśnie irlandzki organ nadzorczy.

Co na to organ?

Irlandzki organ przedstawia swoje wytyczne, w których informuje administratorów danych osobowych o następujących środkach minimalizujących ryzyko naruszenia danych osobowych. Dla zwiększenia czytelności zalecenia organu podzieliłem na kilka grup.

Pracownicy a zabezpieczenia pamięci USB

- Czy pracownik może korzystać z prywatnych urządzeń?
- W żadnym wypadku!

I na tym można zakończyć wszelkie dywagacje. Urząd ujął podejście do prywatnych urządzeń w kilku następujących punktach:

1) zakaz korzystania i podpinania do komputerów służbowych prywatnych pamięci przenośnych pracowników,
2) zakaz zgrywania danych osobowych na prywatne urządzenia przenośne,

3) należy korzystać z autoryzowanych pamięci przenośnych autoryzowanych przez pracodawcę
4) zakaz korzystania ze służbowych urządzeń przenośnych na prywatnych komputerach,

Powyższe zakazy wydają się rygorystyczne, ale mają swoje uzasadnienie. Żadne złośliwe oprogramowanie nie powinno dostać się na przenośną pamięć, jeżeli jest ona używana jedynie w zamkniętym środowisku pracodawcy. Dodatkowo pamiętajmy o zrobieniu spisu posiadanych aktywów, czyli prowadzeniu ewidencji posiadanych pamięci masowych, oraz o aktualizowaniu tego rejestru w przypadku wydania nośnika lub jego zwróceniu przez pracownika.

W swoich zaleceniach organ jeszcze kilkukrotnie wspomina o pracownikach. Mianowicie:

1) należy ograniczyć liczbę pracowników mogących zgrywać pliki na pamięci zewnętrzne,
2) każdy z pracowników musi posiadać aktualne upoważnienie oraz zobowiązanie do poufności,
3) każde urządzenie powinno mieć przypisanego swojego użytkownika, który jest odpowiedzialny za daną pamięć,
4) każdy pracownik po zakończeniu pracy musi zwrócić urządzenie.

Zabezpieczenia techniczne.

Jeżeli chodzi o zabezpieczenia techniczne, to urządzenia przenośne powinny być:

1) zaszyfrowane (cały dysk), oraz
5) zabezpieczone hasłem.

Co możemy uznać za silne hasło? Zgodnie z zaleceniami hasło powinno składać się z co najmniej dwunastu znaków i zawierać co najmniej jeden z następujących elementów: mała bądź duża litera, cyfra lub znak specjalny.

Dodatkowo trzeba mieć na uwadze, aby:

1) pracownik mógł zgrywać dane na pamięci masowe tylko na krótki okres, a jeżeli to możliwe, powinien być wdrożony system, który automatycznie usuwa danym po konkretnym czasie,
2) pracownik usuwał dane z pamięci przenośnej, gdy są już zbędne,
3) była możliwość (o ile to wykonalne) zdalnego usunięcia danych (na odległość) z pamięci pracownika,
4) robić kopię przeniesionych danych na pamięć, aby w przypadku zgubienia urządzenia była możliwość ich odtworzenia,
5) pamięci masowej nie pozostawiać bez nadzoru (w szczególności podczas transportu), a nieużywana pamięć powinna być zabezpieczona (np. przechowywana w bezpiecznym pomieszczeniu/szufladzie),
6) IT dokonywało przeglądów pamięci przenośnych w celu upewnienia się, że są przechowywane na nim jedynie dopuszczalne dokumenty (bez nielegalnych programów/materiałów),
7) urządzenia pochodziły od renomowanych dostawców.

Podsumowanie. Zwiększ świadomość pracowników i szyfruj pamięć!

Powyższe zasady oczywiście należy wdrożyć w firmie w postaci wewnętrznej polityki zawierającej wymienione zalecenia i zakomunikować je całemu personelowi. Świadomość od zawsze jest najważniejsza, ponieważ do większości naruszeń dochodzi z powodu błędu osoby, będącej najbardziej związanej z administratorem danych – czyli z winy pracownika.

Dlatego każdy pracodawca musi pamiętać o zapewnieniu szkoleń dla pracowników (i to nie jednorazowych, a wielokrotnie przypominać pracownikom o zasadach bezpieczeństwa!) w celu szerzenia wiedzy z wdrożonych procedur, bezpiecznego postępowania z nośnikami pamięci, czy możliwych niebezpieczeństw, które mogą spowodować negatywne konsekwencje wobec organizacji.
Natomiast jeżeli dojdzie do naruszenia, bez znaczenia czy z powodu zwykłego ludzkiego błędu bądź zuchwałej kradzieży, musimy mieć pewność, że technologia nas nie zawiedzie. W końcu, jeżeli dane były szyfrowane mocnym hasłem, to zgodnie z wytycznymi irlandzkiego urzędu, może nie będzie konieczności zgłaszania naruszenia bezpieczeństwa danych (2). Dlatego dla każdej firmy najcenniejszym aktywem jest świadomy pracownik, a następnie równie ważne jest mocne zabezpieczenie techniczne.

Źródło:

(1) https://www.dataprotection.ie/en/dpc-guidance/general-portable-storage-device-recommendations
(2) https://dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide

Przemysław Siarka – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.