Przykłady najczęściej spotykanych incydentów oraz ich zapobieganie

Nowy Rok to czas, w którym warto poruszyć kwestie zapewnienia bezpieczeństwa przetwarzanych przez Państwa danych osobowych. Jest to okres, w którym po zakończonych urlopach wracamy do pracy. Pamiętajmy, że jesteśmy odpowiedzialni za bezpieczeństwo danych osobowych, do których mamy dostęp i na których pracujemy.

W związku z powyższym zwracam się do Państwa z ogromną prośbą o czujność oraz przypomnienie sobie procedur związanych z bezpiecznym korzystaniem zarówno z poczty elektronicznej, jak i sieci Internet. Poniżej przedstawiam Państwu przykłady najczęściej występujących naruszeń oraz informacje jak takim naruszeniom zapobiegać. Wszystkie poniżej wymienione sytuacje nie powinny mieć miejsca, a niestety, miejsce mają często ze względu na pośpiech, nieprzestrzeganie procedur, zbytnią ufność w dobre intencje innych.

Poniżej lista najczęściej spotykanych incydentów bezpieczeństwa:

1. E-mail (lub pismo) wysłane na niewłaściwy adres – częsty błąd wynikający najczęściej z trzech czynników: pierwszy to brak podwójnej weryfikacji zgodności adresu mailowego, drugi to błąd ludzki polegający na dodaniu znaku interpunkcyjnego lub ostatni, przekazany błędny adres ze strony właściciela danych.

2. Błędna dokumentacja w wysyłanej korespondencji – pośpiech nigdy nie jest naszym sprzymierzeńcem, zanim zakleimy kopertę zweryfikujmy podwójnie jej zawartość wraz z adresem nadania.

3. Naruszenia związane z niewłaściwym zabezpieczeniem od strony IT, w tym ataki hackerskie – wynikające z braku ostrożności w trakcie weryfikacji przez pracownika korespondencji elektronicznej (kliknięcie w link, przekazanie danych, pobranie niebezpiecznych załączników). W razie wystąpienia wątpliwości co do przesłanego linku czy załącznika, najlepiej wiadomosc taką skonlultować z działem IT. Proszę o zwrócenie szczególnej uwagi na tego typu wiadomości, nieklikanie w linki, a wpisywanie adresów ręcznie.
Najpopularniejszymi technikami służącymi pozyskiwaniu poufnych danych od użytkowników są metody wyłudzania danych zwane phishingiem. Jedną z form phishingu jest przesyłanie wiadomości, które rzekomo pochodzą z godnych zaufania źródeł np. banków, portali społecznościowych. W tego rodzaju wiadomościach umieszczany jest link, po kliknięciu którego użytkownik (przekonany, że znajduje się na oryginalnej witrynie) – odwiedza fałszywą stronę www i wprowadza wymagane informacje. Do tego celu wykorzystywane są grafiki znanych firm, stopki maila, nazwiska osób pracujących w danym podmiocie. Fałszywe wiadomości email kierują użytkowników na witryny www, które wyglądem przypominają witryny znanych firm. W rzeczywistości zarówno zawartość, jak i adres www są sfałszowane. Po kliknięciu w przesłany link przenoszeni są Państwo na ww. stronę. Brak jest jednak protokołu bezpieczeństwa, sam adres strony nieznacznie się różni (np. zamiast mbank.pl link to rnbank.pl).

4. Zagubienie przez pracowników dokumentów – wynikające najczęściej z braku prowadzenia ewidencji wynoszonych dokumentów przez pracowników poza organizację. Najlepszym sposobem zapobiegania takim sytuacjom jest transportowanie dokumentów jedynie z punku A do punktu docelowego B. Każda zmiana trasy czy dodatkowy przystanek stwarza zagrożenie zagubienia transportowanej dokumentacji.

5. Zagubienie przez pracowników pamięci typu pendrive, na którym znajdują się dokumenty zawierające dane osobowe. Naruszeniu można zapobiegać - metodą wprost preferowaną przez RODO, zalecaną przez UODO, w tym przypadku jest szyfrowanie danych. Pendrive powinien być zatem chroniony rozwiązaniem szyfrującym które sprawi, że urządzenie jest nieczytelne dla osoby postronnej. Z kolei

dostęp do danych może weryfikować usługa podwójnego uwierzytelniania, dzięki któremu osoba chcąca skorzystać z nośnika otrzyma hasło do danych np. w formie SMS. Wystarczy skorzystać z odpowiedniego programu. Dzięki temu przypadkowy „znalazca" urządzenia nie będzie miał dostępu do znajdujących się na nim danych.

6. Niewłaściwa anonimizacja danych osobowych – często darzymy zaufaniem niewłaściwe osoby – nie szyfrujemy danych przy wysłaniu lub nie anonimizujemy ich, choć podejrzewamy, że odbiorca nie powinien mieć do nich dostępu. Zawsze warto zaszyfrować załącznik, którym są dane osobowe. Hasło do rozpakowania pliku przesyłamy np. za pośrednictwem SMS.

7. Udostępnianie nagrań z monitoringu – zdarza się, że dla „polubownego" załatwienia spraw publikujemy nagrania na stronach www celem odszukania osób, których wizerunek został na nich utrwalony lub przekazujemy od razu po zgłoszeniu o takie nagranie. Pamiętajmy, że nagrania z monitoringu zawierające dane szczególnych kategorii – w tym przypadku wizerunek osób - możemy udostępnić jedynie podmiotom do tego uprawnionym.
8. Udzielenie informacji osobie nieuprawnionej w trakcie rozmowy telefonicznej - niezweryfikowanie tożsamości osoby dzwoniącej za pomocą pytania kontrolnego. Pamiętajmy, że zwykle nie mamy pewności co do osoby, która znajduje się po drugiej stronie słuchawki. Przed udzieleniem informacji warto takiego rozmówcę zweryfikować.