25.05.2018

KRAJOWE BIURO OBSŁUGI ROSZCZEŃ UBEZPIECZENIOWYCH®

RODO

Przykłady skutecznego wykorzystania przygotowanej przez nas polisy ubezpieczeniowej w kontekście Rozporządzenia RODO:

I.ODPOWIEDZIALNOŚĆ CYWILNA ZA NARUSZENIE PRYWATNOŚCI:

Na terenie niewielkiego zakładu utylizacji odpadów pracownicy znaleźli karty pacjentów miejscowego ośrodka zdrowia. Zawierały one nazwiska i pełną historię medyczną - czyli dane wyjątkowo wrażliwe. Sprawa została nagłośniona przez lokalne media i spowodowała ogromne wzburzenie opinii publicznej.

Osoby, których dane zostały ujawnione zgłosiły roszczenie przeciwko placówce medycznej o naruszenie dóbr osobistych oraz naruszenie tajemnicy lekarskiej.

II. ODPOWIEDZIALNOŚĆ ADMINISTRACYJNA ZA NARUSZENIE PRYWATNOŚCI:

W jednym z portali internetowych doszło do kradzieży danych kont pocztowych wraz z częścią korespondencji użytkowników.
Zarząd spółki prowadzącej portal sam powiadomił o tym organy ścigania oraz Urząd Ochrony Danych Osobowych. Na podstawie zawiadomienia Urząd wszczął kontrolę, która wykazała liczne uchybienia i zaniedbania w zakresie środków technicznych i organizacyjnych, służących bezpieczeństwu przetwarzanych danych.
Skutkowało to zastosowaniem wobec spółki – właściciela portalu – przewidzianych prawem środków administracyjnych. Na spółkę nałożono obowiązek poprawy procedur bezpieczeństwa. Gdyby nowe przepisy RODO już działały – uchybienia te skutkowałyby nałożeniem kary administracyjnej w wysokości kilkudziesięciu tysięcy złotych.

III. KOSZTY OBSŁUGI INCYDENTU INFORMATYCZNEGO:

Atak hakerski na system sterujący pracą magazynu i obsługą zamówień średniej wielkości fabryki spowodował całkowite zatrzymanie produkcji.
Tym samym firma nie była w stanie zrealizować zamówień odbiorców, co spowodowało nie tylko straty finansowe, ale też ogromy uszczerbek na wizerunku.
W celu przywrócenia dostępu do systemu, a w konsekwencji wznowienia produkcji, zakład zmuszony był skorzystać z usługi informatyki śledczej. Ponadto musiał zatrudnić czołową agencję PR, która natychmiast podjęła tzw. „monitoring zaufania" kontrahentów i klientów oraz kosztowne, aczkolwiek niezbędne działania wizerunkowe.

22 256 53 00 biuro@kboru.pl www.kboru.pl

IV. ODPOWIEDZIALNOŚĆ CYWILNA ZA NARUSZENIE BEZPIECZEŃSTWA INFORMACJI U OSÓB TRZECICH:

Urząd Gminy ma dostęp on-line do centralnej bazy PESEL. Wymiana informacji między urzędem a bazą następuje poprzez „wtyczki" zainstalowane na stacjach roboczych urzędu. Zgodnie z wytycznymi RODO urząd ma obowiązek „wdrożenia technicznych i organizacyjnych środków gwarantujących bezpieczeństwo" tych danych.
Jeden z urzędników po zakończeniu pracy nie wylogował się z bazy centralnej, co spowodowało, że osoby trzecie miały dostęp do przechowywanych w nim informacji skutkujący wyciekiem dużej ilości danych osobowych.
Administrator bazy centralnej wystąpił do urzędu z roszczeniem za naruszenie bezpieczeństwa informacji.

V. ODPOWIEDZIALNOŚĆ MULTIMEDIALNA:

Sklep internetowy specjalizował się w sprzedaży suplementów diety i lekarstw bez recepty. Do promocji produktów używał m.in. swojego konta na Facebooku. Korzystał przy tym z różnych grafik, zdjęć oraz fragmentów wypowiedzi znanych autorytetów z danej dziedziny medycyny.
Wobec firmy zostały skierowane dwa roszczenia. Pierwsze od autora badań, którego wyniki były publikowane na koncie w celu potwierdzenia jakości oferowanego produktu. Drugie od fotografa, którego zdjęcie było wykorzystane do promocji konta. Żaden z nich nie był zapytany przez sklep o zgodę na wykorzystanie tych materiałów. Oba roszczenia opiewały na kwotę blisko 100 000 zł.

VI. KOSZTY CYBER-WYMUSZENIA:

W średniej wielkości biurze rachunkowym w połowie stycznia doszło do włamania do systemu księgowego, z którego korzystało biuro i zablokowania dostępu do znajdujących się tam danych.
Haker zażądał „okupu" za przywrócenie dostępu w wysokości 500 USD (płatne Bitcoinem). Właścicielka biura zgłosiła ten fakt do Ubezpieczyciela, który na podstawie analizy sytuacji i ryzyka roszczeń za nierozliczone w terminie operacje podatkowe zgodził się na refundację kosztu.

VII. KOSZTY ODTWORZENIA DANYCH I UTRACONY ZYSK:

Atak hakerski (typu ransomware) na sklep internetowy z ekologicznymi kosmetykami doprowadził do zaszyfrowania danych w systemie zamówień i rozliczeń. Spowodowało to brak możliwości rejestracji zakupów i realizacji płatności, a tym samym przerwę w działalności skutkującą utratą zysku.
Haker zażądał 1000 USD (płatnych Bitcoinem) za przywrócenie dostępu do systemu i odszyfrowanie danych. Właściciel odmówił zapłaty i złożył zawiadomienie do prokuratury. Blokada systemu spowodowała konieczność zamknięcia na pewien czas witryny w celu jej lepszego zabezpieczenia, odtworzenia danych oraz zaktualizowania statusu zamówień.