**Klinika ukarana grzywną 3 mln dolarów w pięć lat po wycieku danych pacjentów**

**Sprawa wycieku danych, do którego doszło pięć lat temu, powraca i uderza w centrum medyczne z Tennessee grzywną w wysokości kilku milionów dolarów.**

Touchstone Medical Imaging, amerykańska firma medyczna świadcząca usługi z zakresu diagnostyki obrazowej, została ukarana przez Biuro Praw Obywatelskich (dalej BPO) Departamentu Zdrowia i Opieki Społecznej USA (dalej ZOS) grzywną w wysokości 3 milionów dolarów po tym, jak analitycy doszli do wniosku, że w klinice miały miejsce zaniedbania w ochronie dokumentacji medycznej pacjentów.

Zgodnie z komunikatem prasowym ZOS, w maju 2014 r. FBI i BPO powiadomiły Touchstone, że z serwerów firmy miał miejsce wyciek informacji o zdrowiu pacjentów (ang. Patient Health Information – PHI).

„Ten niekontrolowany dostęp do dokumentacji medycznej pozwolił wyszukiwarkom indeksować PHI pacjentów, czego ślady pozostały widoczne w internecie nawet po wyłączeniu serwera” – wynika z raportu.

W obliczu tych oskarżeń Touchston początkowo zaprzeczył, jakoby dokumentację medyczną eksponował na zewnątrz. Jednakże późniejsze dochodzenie ujawniło, że w przypadku ponad 300 tys. rekordów firma faktycznie popełniła błąd, ujawniając w sieci imiona i nazwiska, daty urodzenia, numery ubezpieczenia społecznego i adresy zamieszkania pacjentów.

- *Podobno Touchstone potrzebował „kilku miesięcy” na samo rozpoczęcie badań wycieku, przez tak długi czas pozostawiając pacjentów narażonych na oszustwa, szantaż i inne rodzaje ryzyka, grożące ze strony hakerów mających dostęp do tych poufnych danych* - **tłumaczy Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl).

„Dochodzenie BPO wykazało ponadto, że Touchstone nie przeprowadził starannej i gruntownej analizy ryzyka, jakie wiąże się z potencjalnym wyciekiem poufnych danych, jak również nie dokonał oceny integralności i zabezpieczeń całej elektronicznej dokumentacji medycznej. Klinika nie zawarła też biznesowych umów stowarzyszeniowych ze swoimi kooperantami, takimi jak firma udzielająca wsparcia IT i zewnętrzny dostawca usług z zakresu przetwarzania danych, jak tego wymaga ustawa HIPAA” – napisał ZOS.

Oprócz zapłaty grzywny w wysokości 3 mln USD, Touchstone otrzymał polecenie realizacji „solidnego planu działań naprawczych”, w tym analizy ryzyka w skali całego przedsiębiorstwa. W chwili pisania tego tekstu strona internetowa kliniki była niedostępna.