CYBERBEZPIECZEŃSTWO
w placówce medycznej

WIEDZA I PRAKTYKA

Cyberbezpieczeństwo w placówce medycznej

Autorzy:

Piotr Glen
inspektor ochrony danych, ekspert ds. ochrony danych osobowych, audytor systemów zarządzania bezpieczeństwem informacji

Michał Grabiec
radca prawny, kancelaria GW Legal Grabiec & Wójcik sp. p.

Piotr Janiszewski
radca prawny. Audytem w obszarze ochrony danych osobowych zajmuje się od lat. Doświadczony były Administrator Bezpieczeństwa Informacji i trener. Certyfikowany audytor wewnętrzny według normy ISO 27001. Uczestnik inspekcji oraz postępowań administracyjnych prowadzonych przez organ nadzorczy. Autor licznych artykułów i opracowań dotyczących tematyki ochrony danych osobowych. Ekspert w zakresie informacji publicznej i tajemnicy przedsiębiorstwa

Agnieszka Kręcisz-Sarna
radca prawny, specjalista z zakresu ochrony danych osobowych

Przemysław Kucharzewski
VP Sales w Cypherdog – producent rozwiązań cyberbezpieczeństwa. Członek ISSA Polska, Rady Biznesu WSH. Od 25 lat w branży IT, związany z dystrybucją przez blisko 20 lat (JTT Computer, Incom, AB, Eptimo), Interim Manager u integratorów i producentów rozwiązań IT (Xopero, Newind), skupiony na budowie świadomości z zakresu cyberzagrożeń i rozwijania kanałów sprzedaży rozwiązań z obszaru cyberbezpieczeństwa

Maciej Lipka
prawnik i specjalista ds. danych osobowych, były pracownik departamentów skarg, legislacji i prasowego w Urzędzie Ochrony Danych Osobowych; na bazie swojego doświadczenia doradza, jak dostosować organizację do aktualnych przepisów oraz zdarzeń mających wpływ na przetwarzanie danych

Michał Nosowski
radca prawny, specjalizujący się w prawie nowych technologii i ochronie danych osobowych. www.michalnosowski.pl, www.wsroddanych.pl

Marzena Pytlarz-Pietraszko
radca prawny, absolwentka Wydziału Prawa i Administracji oraz studiów podyplomowych „Prawa gospodarczego i handlowego" Uniwersytetu Śląskiego w Katowicach. Uczestniczka studiów podyplomowych „Prawa medycznego i bioetyki" organizowanych na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie. Kierownik działu prawnego w Centrum Nowoczesnej Rehabilitacji i Opieki TriVita, właściciel PCC Legal

Marcin Sarna
radca prawny, ekspert z zakresu ochrony danych osobowych. Specjalizuje się również w kompleksowej obsłudze prawnej podmiotów gospodarczych, w szczególności świadcząc pomoc prawną dla producentów maszyn i urządzeń, przedsiębiorców funkcjonujących w branży usługowej i w sektorze energetycznym

Jowita Sobczak
inspektor ochrony danych, doktor nauk prawnych, specjalista z zakresu ochrony danych osobowych, były ekspert w komisji do spraw reformy prawa ochrony danych osobowych w Unii Europejskiej w Biurze Generalnego Inspektora Ochrony Danych Osobowych

Redaktor: **Michał Kowalski**
Menedżer produktu: **Anna Konarzewska-Żuczek**
Segment manager: **Alina Sulgostowska**
Projekt graficzny okładki: **Piotr Fedorczyk**
Korekta: **Zespół**
Koordynator produkcji: **Magdalena Huta**
Druk: **KRM Druk**
Skład i łamanie: **Triograf Dariusz Kołacz**
ISBN 978-83-8276-286-0

Warszawa 2022
Wiedza i Praktyka sp. z o.o.
ul. Łotewska 9a, 03-918 Warszawa,
tel. 22 518 29 29, faks 22 617 60 10, e-mail: cok@wip.pl
NIP: 526-19-92-256, KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy w Warszawie,
XIII Wydział Gospodarczy Krajowego Rejestru Sądowego,
wysokość kapitału zakładowego 200.000 zł,
nr rejestrowy BDO: 000008579.

Publikacja „Cyberbezpieczeństwo w placówce medycznej" została przygotowana z zachowaniem najwyższej staranności i wykorzystaniem wysokich kwalifikacji, wiedzy oraz doświadczenia jej twórców. Zaproponowane w niej wskazówki, porady i interpretacje dotyczą sytuacji typowych. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Opublikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych. W konsekwencji autorzy, konsultanci oraz redakcja nie mogą ponosić odpowiedzialności prawnej za zastosowanie zawartych w publikacji „Cyberbezpieczeństwo w placówce medycznej" wskazówek, przykładów, informacji itp. do konkretnych przypadków.

Szanowni Czytelnicy,

Cyberprzestępczość nie jest obca także służbie zdrowia. Coraz częściej można bowiem spotkać się z próbami cyberataków na placówki medyczne. Niestety bywają one skuteczne, czego przykładem jest choćby niedawny incydent w Instytucie Centrum Zdrowia Matki Polki, który miał miejsce 4 listopada 2022 r. Cyberatak spowodował tam ograniczenia w funkcjonowaniu systemu IT, co z kolei przełożyło się na trudności w udzielaniu świadczeń zdrowotnych.

Przykład ten doskonale pokazuje, że atak na system IT placówki medycznej może sparaliżować jej funkcjonowanie. Poza tym placówki narażają się na kary administracyjne z powodu niedostatecznych zabezpieczeń, które mogą stanowić znaczne obciążenie dla ich budżetu.

Właśnie ze względu na narastające zagrożenie cyberprzestępczością w służbie zdrowia oddajemy w Wasze ręce I wydanie publikacji „Cyberbezpieczeństwo w placówce medycznej". W publikacji poruszamy najważniejsze zagadnienia tego aspektu działalności placówek. Poza omówieniem popularnych rodzajów cyberataków znajdziecie w niej praktyczne wskazówki dotyczące zabezpieczeń:

- systemów IT i oprogramowania,
- poczty e-mail,
- serwerów i sieci lokalnej.

Nie zabrakło także zagadnień specyficznych dla służby zdrowia, a mianowicie:

- systemu Zarządzania Bezpieczeństwem Informacji (oraz innych obowiązków placówek medycznych jako operatorów usług kluczowych),
- bezpieczeństwa dokumentacji medycznej,
- teleporad.

To wszystko okraszone zostało wzorami dokumentów i listami kontrolnymi, pomocnymi w organizacji zabezpieczeń w placówce.

Życzę owocnej lektury.

Michał Kowalski

radca prawny, redaktor publikacji

SPIS TREŚCI

ROZDZIAŁ 1. RODZAJE CYBERATAKÓW W PLACÓWKACH MEDYCZNYCH

Cyberatak stanowi działanie ukierunkowane na komputer lub jakikolwiek element komputerowego systemu informatycznego, mające na celu zmianę, zniszczenie lub kradzież danych albo wykorzystanie lub uszkodzenie sieci. Liczba cyberataków wzrasta wraz z postępującą cyfryzacją w działalności placówek medycznych, tj. przechowywania przez nie coraz większej ilości informacji w postaci zapisu komputerowego. Chociaż istnieją setki różnych rodzajów ataków, najpopularniejsze z nich można skatalogować według podobieństwa. Wiedza o poszczególnych rodzajach cyberataków jest kluczowa dla ich rozpoznawania i właściwej reakcji. Pomaga też wdrożyć odpowiednie zabezpieczenia.

1.1. Malware

Malware to ogólne pojęcie określające złośliwe oprogramowanie, które infekuje komputer i zmienia sposób jego działania w sposób zaplanowany przez atakującego: najczęściej niszczy dane lub szpieguje użytkownika. Malware może rozprzestrzeniać się z jednego urządzenia na drugie, ale też pozostawać na swoim miejscu, wpływając tylko na urządzenie gospodarza. Co istotne, aby malware zadziałało, musi dojść do działania ze strony użytkownika. Oprogramowanie musi bowiem zostać zainstalowane na urządzeniu docelowym.