

CYBERBEZPIECZEŃSTWO

w placówce medycznej



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 (JIT 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 departamentu 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 bietyki” 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

Copyright by Wiedza i Praktyka sp. z o.o.

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 popularnych w placówkach medycznych	7
1.1. Malware	7
1.2. DoS i DDoS	8
1.3. Man-in-the-middle (MITM)	9
1.4. Phishing	9
1.5. Ransomware	12
1.6. Invoice hacking	12
1.7. Spoofing	13
1.8. Skimming	14
1.9. Oszustwo nigeryjskie	15
1.10. Jak reagować na cyberataki – wskazówki ogólne	15
Rozdział 2. Bezpieczeństwo oprogramowania i systemów IT w placówce medycznej	17
2.1. Jak wybrać właściwe technologie	17
2.2. Swoboda, ale nie dowolność	18
2.3. Najpierw analiza ryzyka	20
2.4. Warto postawić na sprawdzone rozwiązania	20
2.5. Czym kierować się, wybierając oprogramowanie	22
2.6. Koszty mogą być brane pod uwagę	24
2.7. Zarządzanie podatnościami w kontekście IT	25
2.8. Czy warto opracować instrukcję zarządzania systemem IT	26
2.9. Konieczne regularne testowanie zabezpieczeń	28
2.10. Należy sprawdzić wiedzę personelu	28
2.11. Audyt systemu IT	30
2.12. Wskazówki UODO	32
Rozdział 3. Bezpieczna poczta elektroniczna w placówce medycznej	33
3.1. W pierwszej kolejności analiza ryzyka	33
3.2. 6 zabezpieczeń poczty e-mail	35
3.3. Przede wszystkim szyfrowanie	36
3.4. Warto skorzystać z uwierzytelniania dwuskładnikowego	38
3.5. Dlaczego warto opracować politykę haseł	38
3.6. A może monitoring poczty e-mail	40
3.7. Monitoring nie może obejmować prywatnego e-maila	41
3.8. Wskazówki UODO	42

Rozdział 4. Bezpieczne serwery i sieć lokalna	45
4.1. Najpierw należy wyznaczyć obszary bezpieczeństwa	45
4.2. Należy zabezpieczyć pomieszczenia krytyczne	46
4.3. Należy zabezpieczyć także gabinety	47
4.4. Więcej źródeł zasilania	48
4.5. Jak walczyć z atakami typu DoS i DDoS	49
4.6. Audyty bezpieczeństwa w celu ochrony serwerów	51
4.7. Monitoring sieci lokalnej	51
4.8. Zasada „zero zaufania” – czy warto ją wdrożyć	53
4.9. Kopie zapasowe – przymus czy dobra praktyka	55
4.10. Jak stosować kopie zapasowe	57
4.11. Jak często tworzyć kopie zapasowe	58
4.12. Jak i gdzie przechowywać kopie zapasowe	59
Rozdział 5. SZBI w publicznej placówce medycznej i inne obowiązki w krajowym systemie cyberbezpieczeństwa	61
5.1. SZBI – co to takiego	62
5.2. Jak utworzyć i aktualizować SZBI	62
5.3. 9 obowiązków w zakresie SZBI	63
5.4. Audyt SZBI – polskie normy	64
5.5. Konieczne zgłaszanie incydentów do CSIRT	66
5.7. Zarządzanie incydemem	67
5.8. Pacjenci muszą być poinformowani o incydencie	68
5.9. Pozostałe obowiązki placówki medycznej jako operatora usługi kluczowej	68
Rozdział 6. Bezpieczna dokumentacja medyczna w postaci elektronicznej	71
6.1. Co grozi za utratę dokumentacji medycznej	71
6.2. Jak zabezpieczyć dokumentację elektroniczną	72
6.3. Dokumentacja medyczna a system IT	74
Rozdział 7. Bezpieczna teleporada	75
7.1. Kilka słów o teleporadzie	76
7.2. Priorytetem bezpieczne dane pacjenta	76
7.3. Należy spełnić standardy organizacyjne teleporady	77
7.4. Bezpieczna rejestracja medyczna pacjenta	78
7.5. Należy chronić wizerunek pacjenta	80
7.6. Jak przekazać dokumentację z teleporady pacjentowi	81
7.7. Teleporada a dane pacjenta na poczcie e-mail	82
7.8. Bezpieczna teleporada a korzystanie ze smartfonów	84

7.9. 6 rozwiązań zabezpieczających przed cyberatakami w związku z udzielaniem teleporad	87
Rozdział 8. Procedury, listy kontrolne i wzory dokumentów	
przydatne dla placówki medycznej	89
8.1. Instrukcja zarządzania systemami IT	89
8.2. Plan ciągłości działania	101
8.3. Ewidencja napraw, przeglądów i konserwacji systemu IT	105
8.4. Ewidencja czynności w systemie IT	106
8.5. Polityka haseł	106
8.6. Ewidencja haseł	108
8.7. Regulamin bezpiecznego używania urządzeń przenośnych	109
8.8. Karta oceny incydentu pod kątem wystąpienia naruszenia ochrony danych osobowych	115
8.9. Zawiadomienie podmiotów danych o naruszeniu ochrony danych	118
8.10. Raport z naruszenia ochrony danych	119
8.11. Rejestr naruszeń ochrony danych	120
8.12. Procedura odtwarzania systemów po awarii i ich testowania	121
8.13. Protokół odtwarzania systemu po awarii i testowania	122
9.14. Wytyczne dla personelu placówki medycznej dotyczące cyberbezpieczeństwa	124
9.15. Pakiet checklist dla placówki medycznej	128
Checklista 1. Sprawdź swoją wiedzę na temat cyberbezpieczeństwa	128
Checklista 2. Czy Twój system IT spełnia wymogi RODO	129
Checklista 3. Czy należycie zabezpieczasz elektroniczne nośniki z danymi osobowymi	135
Checklista 4. Czy właściwie analizujesz ryzyko	136
Checklista 5. Czy udostępniasz dokumentację medyczną zgodnie z RODO	139
Checklista 6. Czy zapewniasz bezpieczeństwo danych przechowywanych w aplikacjach klasy EDM	140
Checklista 7. Czy zapewniasz bezpieczną wideokonferencję (teleporadę)	142
Checklista 8. Czy odpowiednio zabezpieczasz prywatne urządzenia mobilne służące do przetwarzania danych	145
Checklista 9. Czy zabezpieczasz dane przekazywane za pośrednictwem poczty elektronicznej	146
Rozdział 9. Wykaz aktów prawnych, na które powołano się w publikacji	147

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 zadziało, musi dojść do działania ze strony użytkownika. Oprogramowanie musi bowiem zostać zainstalowane na urządzeniu docelowym.