ZODIAC
Zespół Ochrony Danych i Analizy Cyberzagrożeń

małopolskie parki zdrowia Sp. z o.o.

BIULETYN BEZPIECZEŃSTWA

WYDANIE 1/2026

Biuletyn Bezpieczeństwa

Nr 1/2026 (Marzec 2026)

Temat przewodni: „Cybernetyczni zakładnicy: Broń się przed ransomware”

Wprowadzenie: Stare zagrożenia i nowe wyzwania

Marzec to czas, gdy zima powoli odpuszcza, a my nabieramy tempa po pierwszych tygodniach nowego roku. To także dobry moment, by spojrzeć na to, co 2026 przynosi w świecie cyberbezpieczeństwa. A dzieje się sporo — bo przestępcy nie mają przerwy ani ferii zimowych.

Witaj w trzecim numerze *Biuletynu Bezpieczeństwa*! Tym razem przyglądamy się tematowi, który budzi grozę nie tylko wśród informatyków i specjalistów od cyberbezpieczeństwa – ransomware. To złośliwe oprogramowanie, które potrafi zaszyfrować dane i zażądać okupu za ich odzyskanie. Niestety, w ostatnich latach stało się ono prawdziwym utrapieniem sektora ochrony zdrowia.

Statystyki nie pozostawiają złudzeń – szpitale należą do najczęściej atakowanych instytucji. Przestępcy dobrze wiedzą, że placówki medyczne nie mogą sobie pozwolić na przestój systemów, a dane pacjentów to niezwykle cenna zdobycz. Gdy ransomware unieruchamia systemy diagnostyczne, blokuje dostęp do

dokumentacji czy planów operacyjnych, w grę wchodzi nie tylko bezpieczeństwo danych, ale i zdrowie, a nawet życie pacjentów.

Jest jednak dobra wiadomość – przed ransomware można się skutecznie bronić. Co więcej, wiele ataków udaje się tylko dlatego, że ktoś kliknął w podejrzany link, otworzył nieznany załącznik albo użył prostego hasła. To oznacza, że każdy z nas – niezależnie od stanowiska – ma realny wpływ na bezpieczeństwo całego szpitala.

W tym numerze wyjaśnimy, czym dokładnie jest ransomware i jak działa; pokażemy, jak zazwyczaj trafia do naszych systemów i co możemy zrobić, by go powstrzymać. Podpowiemy też, jak postępować, jeśli mimo wszystko dojdzie do incydentu.

Zapraszamy do lektury – i do wspólnego dbania o cyfrowe bezpieczeństwo naszych pacjentów i naszych szpitali.

Czym właściwie jest ransomware i dlaczego szpitale są na jego celowniku?

Ransomware to jedno z najgroźniejszych narzędzi w arsenale cyberprzestępców. Po dostaniu się do komputera lub sieci, taki program błyskawicznie szyfruje wszystkie dane, przez co stają się one całkowicie niedostępne. Chwilę później na ekranie pojawia się komunikat z żądaniem zapłaty – zazwyczaj w kryptowalucie – w zamian za możliwość odzyskania dostępu. Sama nazwa „ransomware" pochodzi od angielskiego słowa *ransom*, czyli okup. Krótko mówiąc: Twoje dane stają się zakładnikami.

Dlaczego właśnie szpitale są na celowniku? Powód jest prosty – każda minuta w ochronie zdrowia ma znaczenie. Placówki medyczne działają bez przerwy, a dostęp do dokumentacji pacjentów, wyników badań i harmonogramów operacji to dla personelu codzienna konieczność. Gdy system przestaje działać, lekarze i pielęgniarki tracą dostęp do kluczowych informacji, a decyzje o leczeniu muszą być podejmowane w trudniejszych warunkach.

Przestępcy dobrze o tym wiedzą. Liczą na to, że w sytuacji presji czasu i odpowiedzialności za pacjentów szpital zechce zapłacić, by jak najszybciej przywrócić pracę systemów. To właśnie ten element presji sprawia, że sektor medyczny stał się dla cyberprzestępców jednym z najbardziej kuszących celów.

Jak wygląda „scenariusz" ataku ransomware?

Atak ransomware rzadko bywa dziełem przypadku. Zwykle to dobrze zaplanowana akcja, która krok po kroku prowadzi do sparaliżowania placówki.

Wejście do środka

Na początku przestępcy muszą jakoś „wejść" do naszej sieci. Często dzieje się to przez wiadomość phishingową z podejrzanym linkiem lub załącznikiem, przez lukę w nieaktualnym oprogramowaniu albo dzięki skradzionym czy zbyt prostym hasłom. Jeden nieostrożny klik może otworzyć im drzwi.

Ciche rozpoznanie terenu

Gdy atakujący znajdą się już w środku, nie spieszą się z działaniem. Złośliwe oprogramowanie po cichu „rozgląda się" po sieci, sprawdza, jakie komputery i serwery są dostępne i gdzie znajdują się najbardziej wrażliwe dane. Taki „rekonesans" może trwać dniami, a nawet tygodniami.

Uderzenie w najgorszym możliwym momencie

Kiedy wszystko jest już przygotowane, przychodzi czas na właściwy atak – często w nocy, w weekend albo w święta, gdy obsada jest mniejsza. Ransomware zaczyna masowo szyfrować pliki, blokując dostęp do systemów i danych. Wtedy na ekranach pojawia się komunikat z żądaniem okupu.

Podwójny szantaż

Coraz częściej przestępcy grają „va banque". Zanim zablokują dane, kopiują je na swoje serwery. Potem grożą, że jeśli szpital nie zapłaci, wrażliwe informacje – w tym dane pacjentów – mogą zostać upublicznione. Tę taktykę nazywa się podwójnym wymuszeniem (ang. *double extortion*).

Zrozumienie, że atak to proces, a nie jedno „nagłe kliknięcie", pomaga lepiej rozpoznawać sygnały ostrzegawcze i reagować, zanim pojawi się komunikat dotyczący okupu na ekranie.

Jak ransomware „wchodzi" do szpitala?

Skoro wiemy już, czym jest ransomware, warto zobaczyć, którędy najczęściej próbuje dostać się do naszych systemów. To trochę jak z bezpieczeństwem budynku: drzwi, okna i brama wjazdowa są różne – i każda z tych dróg wymaga innej czujności.

Phishing – mail, który udaje coś zwyczajnego

Większość ataków zaczyna się od e-maila. Przestępcy potrafią podszywać się pod znane instytucje, dostawców sprzętu, urzędy, a nawet pod naszych współpracowników.

Taki mail często zawiera:

- załącznik udający fakturę, wyniki badań, grafik dyżurów czy dokument z „pilnymi zmianami", który po otwarciu uruchamia złośliwe oprogramowanie,
- link prowadzący do fałszywej strony, gdzie czeka na nas zainfekowany plik albo formularz wyłudzający dane logowania.

Jak się bronić?

1) Sprawdzaj dokładny adres nadawcy, nie tylko wyświetlaną nazwę.
2) Zwracaj uwagę na błędy językowe, nienaturalną pilność („Pilne!", „Natychmiast otwórz!") i niespodziewane załączniki.
3) Gdy coś budzi wątpliwości – nie klikaj, nie otwieraj, tylko skonsultuj się z działem IT lub przełożonym.

Nieaktualne oprogramowanie – uchylone drzwi dla włamywacza

Każdy program ma swoje błędy, które producenci poprawiają w aktualizacjach bezpieczeństwa. Jeśli ich nie instalujemy, zostawiamy atakującym wygodne, dobrze opisane „wejścia" do naszych systemów.

W szpitalu pracuje wiele specjalistycznych aplikacji i urządzeń medycznych, więc utrzymanie wszystkiego w najnowszej wersji bywa wyzwaniem – ale to właśnie od aktualizacji często zaczyna się skuteczna obrona.

Jak się bronić?

1) Nie odkładaj instalacji aktualizacji w nieskończoność – jeśli system prosi o restart, zrób go przy najbliższej możliwej przerwie w pracy.
2) Zgłaszaj do IT problemy ze starym, nieobsługiwanym oprogramowaniem lub urządzeniami, których „wszyscy się boją ruszać".

Słabe i powtarzane hasła

Hasła typu „123456", „haslo", „Szpital2024" czy imię dziecka z datą urodzenia to dla cyberprzestępców praktycznie otwarte konto. Narzędzia do ataków siłowych potrafią automatycznie testować tysiące kombinacji na sekundę.

Jeśli to samo hasło wykorzystujemy w kilku miejscach, włamanie do jednego systemu może otworzyć przestępcom drogę do pozostałych.

Jak się bronić?

1) Używaj długich, unikalnych haseł dla każdego systemu (np. menedżer haseł bardzo to ułatwia).
2) Włączaj wieloskładnikowe uwierzytelnianie (MFA), kiedy tylko jest dostępne.
3) Nie dziel się hasłami – nawet „tylko na chwilę" i „tylko zaufanej osobie".

Nośniki USB i nieautoryzowane urządzenia

Pendrive znaleziony w windzie, prywatny dysk podpięty „na szybko", telefon ładowany z gniazda USB w komputerze – każdy taki nośnik może przenieść złośliwe oprogramowanie. Zdarza się, że przestępcy celowo „podrzucają" zainfekowane pamięci w miejscach, gdzie ktoś może je z ciekawości podłączyć.

Jak się bronić?

1) Nie podłączaj do komputera służbowego urządzeń z nieznanego źródła.
2) Do pracy używaj tylko nośników i kanałów zatwierdzonych przez szpital.
3) Jeśli znajdziesz „bezpański" pendrive lub inne podejrzane urządzenie – przekaż je do działu IT, zamiast sprawdzać jego zawartość na własną rękę.

Każda z tych dróg ataku zaczyna się od drobnej decyzji konkretnej osoby.

Co robić, gdy podejrzewasz atak ransomware?

Wyobraź sobie, że uruchamiasz komputer, a na ekranie zamiast znanego pulpitu pojawia się komunikat z żądaniem okupu. Albo próbujesz otworzyć dokumentację pacjenta, lecz pliki mają dziwne rozszerzenia i nie chcą się otworzyć. W takiej sytuacji najważniejsze są spokój i szybkie, świadome działanie.

Pierwsze kroki — reaguj mądrze i spokojnie

1. **Odłącz komputer od sieci.** Natychmiast wyjmij kabel sieciowy lub wyłącz Wi-Fi. Ransomware może rozprzestrzeniać się błyskawicznie — izolując urządzenie, ograniczasz możliwość zainfekowania kolejnych systemów.
2. **Nie wyłączaj urządzenia.** Wyłączenie komputera może zniszczyć ślady techniczne istotne dla analizy ataku i potencjalnego odzyskania danych. Jeśli dział IT nie zaleci inaczej, zostaw sprzęt włączony, ale odłączony od sieci.
3. **Natychmiast powiadom dział IT.** Zadzwoń lub zgłoś problem przez ustalony kanał. Opisz dokładnie, co widzisz na ekranie, kiedy to zauważyłeś i jakie czynności wykonywałeś. Im więcej informacji przekażesz, tym szybciej specjaliści ocenią sytuację i rozpoczną działania ochronne.

4. **Nie podejmuj żadnych prób zapłaty okupu.** Indywidualni użytkownicy nie powinni wykonywać żadnych transferów ani kontaktować się z przestępcami. Takie decyzje leżą wyłącznie w gestii kierownictwa szpitala we współpracy z zespołem ds. bezpieczeństwa i organami ścigania. Samodzielne działanie może utrudnić odzyskanie danych lub postępowanie dochodzeniowe.
5. **Zabezpiecz dowody.** Jeśli możesz, zrób zdjęcie komunikatu telefonem (nie zrzut ekranu z zainfekowanego urządzenia) i zanotuj dokładny czas wystąpienia problemu. Te informacje pomogą ekspertom w dalszej analizie.

Każdy pracownik — bez względu na stanowisko — odgrywa kluczową rolę w ochronie infrastruktury szpitala. W cyberbezpieczeństwie liczy się nie tylko technologia, ale też szybka reakcja i odpowiedzialne postępowanie.

Czego bezwzględnie nie robić?

1) **Nie próbuj samodzielnie usuwać wirusa** – możesz pogaorszyć sytuację i utrudnić pracę specjalistów.
2) **Nie otwieraj podejrzanych plików na innych komputerach** – możesz rozprzestrzenić infekcję na kolejne urządzenia.
3) **Nie ukrywaj incydentu** – nawet jeśli myślisz, że to może być fałszywy alarm. Każde podejrzenie warto zgłosić – lepiej zareagować raz za dużo niż raz za mało.

Szybka i odpowiedzialna reakcja każdego pracownika może zadecydować o tym, czy atak ransomware zostanie powstrzymany na jednym komputerze, czy też sparaliżuje cały szpital.

Kopie zapasowe – nasza polisa na gorszy dzień

Gdyby trzeba było wskazać jeden element obrony szczególnie ważny w walce z ransomware, byłyby to właśnie kopie zapasowe. Nawet najlepsze zabezpieczenia nie dają stuprocentowej gwarancji, że atak się nie uda, ale dobrze przygotowany backup sprawia, że zamiast płacić okup, możemy po prostu odtworzyć dane i szybciej wrócić do normalnej pracy.

Dlaczego backup jest tak ważny?

Ransomware działa w prosty sposób: szyfruje dane i odcina nas od nich. Jeśli jednak mamy te same informacje zapisane w bezpiecznym, odizolowanym miejscu, szantaż traci sens. Sięgamy po kopię, przywracamy system i kontynuujemy pracę – bez negocjacji z przestępcami.

Co każdy pracownik powinien wiedzieć?

1. **Nie trzymaj wszystkiego „tylko na swoim komputerze".**

   Pliki zapisane wyłącznie na dysku lokalnym mogą zostać zaszyfrowane razem z komputerem. Ważne dokumenty zapisuj na dyskach sieciowych i w zasobach udostępnionych przez dział IT – to one są regularnie obejmowane kopiami zapasowymi.

2. **Nie przerywaj tworzenia kopii zapasowych.**

   Jeśli system informuje o synchronizacji czy wykonywaniu kopii, pozwól mu dokończyć zadanie. Automatyczne backupy wymagają, by komputer był włączony i miał połączenie z siecią o określonej porze.

3. **Zwracaj uwagę na nietypowe zachowanie plików.**

   Jeśli dokumenty znikają, zmieniają nazwy, mają dziwne rozszerzenia albo nagle nie da się ich otworzyć – natychmiast zgłoś to do działu IT. To mogą być pierwsze sygnały działania ransomware i moment, w którym szybka reakcja pozwoli wykorzystać kopie zapasowe, zanim szkody się powiększą.

Dział IT dba o to, by kopie zapasowe były wykonywane regularnie, przechowywane w odseparowanych środowiskach i okresowo testowane pod kątem odtworzenia. Ale bezpieczeństwo to gra zespołowa – technologia to jedno, a świadomość i współpraca wszystkich pracowników szpitala jest równie ważna.

Historia ku przestrodze: jeden klik, który zatrzymał szpital

Ta opowieść jest fikcyjna, ale bardzo podobne scenariusze wydarzyły się już w wielu szpitalach na świecie. Jej bohaterką jest pani Katarzyna – doświadczona oddziałowa, szanowana przez zespół i pacjentów, zorganizowana, zawsze pomocna.

Był poniedziałkowy poranek po długim weekendzie. Pani Katarzyna, zanim ruszyła na obchód, usiadła do komputera, żeby nadrobić pocztę. W skrzynce – dziesiątki wiadomości. Jedna z nich zwróciła jej uwagę: „Pilna aktualizacja – harmonogram dyżurów na marzec". Nadawca wyglądał znajomo – imię i nazwisko koordynatorki, logo szpitala w stopce. W treści krótka prośba o zapoznanie się z załączonym plikiem Excel z „aktualnym grafikiem".

Mail wyglądał wiarygodnie, więc pani Katarzyna nie wczytywała się w szczegóły. Nie zauważyła, że w adresie nadawcy jest jedna dodatkowa litera („szpitall.pl" zamiast „szpital.pl"), a załącznik ma rozszerzenie „.xlsm", które oznacza plik z makrami. Kliknęła. Plik się otworzył, pojawił się krótki komunikat o włączeniu makr – po chwili zniknął. Wszystko wydawało się w porządku.

Tymczasem w tle uruchomił się złośliwy skrypt. Przez kolejne godziny ransomware po cichu rozchodził się po sieci szpitala, szyfrując pliki na kolejnych komputerach i serwerach. Około 14:00 zaczęły pojawiać się pierwsze zgłoszenia: „Nie mogę otworzyć dokumentacji pacjenta", „System strasznie zwalnia", „Co to za dziwny komunikat na ekranie?".

Na ekranach części komputerów pojawił się komunikat po angielsku: „Your files have been encrypted. Pay 50 BTC to restore access." Bardzo podobne komunikaty widziały już wcześniej inne szpitale na świecie, zmuszone do przejścia na papierową dokumentację i przekładania zabiegów. Dział IT ogłosił alarm, odłączono fragmenty sieci, uruchomiono procedury awaryjne i zaczęła się walka o ograniczenie skutków ataku.

Kolejne 48 godzin było bardzo trudne dla całej placówki. Część oddziałów wróciła do dokumentacji papierowej, planowe zabiegi trzeba było przesunąć, a personel pracował pod dużą presją, wiedząc, że dostęp do systemów ma bezpośrednie znaczenie dla bezpieczeństwa pacjentów.

Na szczęście szpital miał aktualne kopie zapasowe w odizolowanym środowisku, dzięki czemu w ciągu kilku dni udało się odzyskać większość danych bez płacenia okupu. Mimo to straty były poważne: koszty odtwarzania systemów, przełożone zabiegi, zakłócone zaufanie pacjentów oraz tygodnie intensywnej pracy działu IT nad pełnym przywróceniem działania infrastruktury.

Najtrudniejszy był dla pani Katarzyny moment uświadomienia sobie, że to jej jedno kliknięcie uruchomiło całą lawinę zdarzeń. Zrozumiała, że wystarczyłoby kilka

sekund więcej: dokładne spojrzenie na adres nadawcy, zwrócenie uwagi na nietypowe rozszerzenie pliku, a przede wszystkim – przesłanie podejrzanego maila do IT zamiast otwierania załącznika.

Ta historia stała się w szpitalu ważnym przypomnieniem, że cyberbezpieczeństwo to nie abstrakcyjne hasło z prezentacji, ale codzienne decyzje podejmowane przy klawiaturze. Każdy z nas – lekarz, pielęgniarka, rejestratorka, informatyk czy członek kierownictwa – może być zarówno pierwszą linią obrony, jak i nieświadomym „wejściem" dla ataku.

Codzienna tarcza anty-ransomware

Ransomware nie bierze urlopu – dlatego nasza obrona też musi działać na co dzień, a nie tylko „od incydentu do incydentu". W poprzednich częściach numeru naszego czasopisma pokazaliśmy, jak wygląda atak i jakie może mieć skutki dla pracy szpitala. Teraz zbierzmy w jednym miejscu najważniejsze zasady, które każdy z nas może stosować przy swoim biurku, stanowisku pielęgniarskim czy w gabinecie. To nie są skomplikowane techniczne procedury, ale proste nawyki, które realnie utrudniają życie cyberprzestępcom.

Poczta elektroniczna i załączniki

1) Nie otwieraj załączników ani nie klikaj linków w wiadomościach od nieznanych nadawców lub takich, które budzą choć cień wątpliwości.

2) Uważnie patrz na rozszerzenia plików – szczególnie .exe, .xlsm, .docm, .zip, .js. To właśnie w takich formatach często ukrywa się złośliwy kod.
3) Podejrzane wiadomości przekaż do działu IT lub zgłoś je zgodnie z przyjętą procedurą – nie usuwaj ich od razu, mogą być potrzebne do analizy i lepszego zabezpieczenia systemów.

Hasła i uwierzytelnianie

1) Korzystaj z silnych, unikalnych haseł – co najmniej 12 znaków, z literami, cyframi i znakami specjalnymi.
2) Włączaj wieloskładnikowe uwierzytelnianie (MFA) wszędzie tam, gdzie jest dostępne – to prosty sposób na dodanie „drugiej kłódki" do konta.
3) Nie udostępniaj swoich haseł innym osobom i nie zapisuj ich w łatwo dostępnym miejscu (np. na karteczce przy monitorze).

Aktualizacje i oprogramowanie

1) Nie odkładaj instalowania aktualizacji systemu i aplikacji „na później". Każda łatka bezpieczeństwa to zamknięcie konkretnej furtki, którą mogą wykorzystać atakujący.
2) Nie instaluj samodzielnie nowego oprogramowania na służbowym komputerze. Korzystaj wyłącznie z aplikacji zatwierdzonych przez dział IT.
3) Jeśli komputer nagle zaczyna mocno zwalniać, pojawiają się nietypowe komunikaty albo pliki zmieniają rozszerzenia czy przestają się otwierać – odłącz urządzenie od sieci i jak najszybciej skontaktuj się z IT.

Reagowanie na incydenty

1) Gdy podejrzewasz atak ransomware: odłącz komputer od sieci (kabel i Wi-Fi), nie wyłączaj urządzenia i natychmiast powiadom dział IT.
2) Nie próbuj „naprawiać" sytuacji na własną rękę, instalując dodatkowe programy czy skanując system przypadkowymi narzędziami z internetu – od tego są procedury i specjaliści.
3) Zanotuj ważne szczegóły: godzinę, kiedy zauważyłeś problem, treść komunikatu na ekranie, ostatnie wykonywane czynności. Te informacje bardzo pomagają w szybkiej analizie zdarzenia.

Stosowanie tych zasad na co dzień jest jedną z najskuteczniejszych form obrony. Ransomware najczęściej wykorzystuje naszą rutynę i pośpiech – im bardziej jesteśmy świadomi, tym trudniej będzie mu „wejść" do naszego szpitala.

Kącik interaktywny – Quiz: Czy uda Ci się obronić przed ransomware?

Czas na krótki test wiedzy! Spróbuj odpowiedzieć na poniższe pytania, a potem sprawdź swoje odpowiedzi. Powodzenia!

Pytanie 1

Otrzymujesz e-mail zatytułowany „Pilna faktura – do opłacenia dziś" z załącznikiem w formacie .zip. Nadawca jest Ci nieznany, ale w treści wiadomości widnieje logo jednego z dostawców szpitala. Co robisz?

a) Otwieram załącznik, bo logo wygląda wiarygodnie – pewnie to prawdziwa faktura, którą trzeba szybko opłacić.

b) Przekazuję e-mail do działu IT z prośbą o weryfikację, nie otwierając załącznika – wolę sprawdzić niż ryzykować.

c) Kasuję wiadomość – skoro nadawca jest nieznany, to na pewno spam.

Pytanie 2

Pracujesz przy komputerze i nagle zauważasz, że kilka plików na dysku zmieniło nazwę – mają teraz dziwne rozszerzenie, np. „.locked", a próba ich otwarcia kończy się błędem. Co robisz?

a) Próbuję zmienić nazwy plików z powrotem na oryginalne – może to jakiś błąd systemu.

b) Restartuję komputer, żeby zobaczyć, czy problem się sam rozwiąże.

c) Odłączam komputer od sieci i natychmiast powiadamiam dział IT – to mogą być objawy działania ransomware.

Pytanie 3

Na parkingu szpitalnym znajdujesz pendrive z naklejką „Grafik dyżurów – kwiecień 2026". Co z nim robisz?

a) Podłączam do swojego komputera, żeby sprawdzić, do kogo należy i ewentualnie zwrócić właścicielowi.

b) Oddaję pendrive do działu IT bez podłączania go do żadnego komputera – to może być pułapka.

c) Zostawiam go tam, gdzie leży – to pewnie czyjś zgubiony pendrive i nie moja sprawa.

Prawidłowe odpowiedzi: 1) b; 2) c; 3) b.

Gratulacje, jeśli wszystkie Twoje odpowiedzi były poprawne – to znak, że wiesz, jak reagować na zagrożenia związane z ransomware. Jeśli coś Cię zaskoczyło, zachęcamy do powrotu do artykułów w tym numerze i odświeżenia kluczowych zasad.

Dziękujemy za lekturę trzeciego numeru Biuletynu Bezpieczeństwa. Mamy nadzieję, że przedstawione tu wskazówki pomogą Państwu jeszcze lepiej chronić pacjentów i szpital przed zagrożeniami ransomware. Pamiętajmy – każdy z nas jest ważnym ogniwem cyberbezpieczeństwa. Jedno ostrożne spojrzenie na podejrzany e-mail, jedno szybkie zgłoszenie do działu IT, jedna chwila refleksji przed kliknięciem – to działania, które mogą ochronić tysiące danych pacjentów i ciągłość pracy całej placówki. Bądźmy czujni – razem jesteśmy bezpieczniejsi!