

Jak chronić dane medyczne przed hakerami? Porady dla personelu medycznego

Autor: Artur Olesch

Ataki na ochronę zdrowia stanowią aż 53 proc. wszystkich incydentów cybernetycznych – wynika z nowych danych Agencji ds. Cyberbezpieczeństwa Unii Europejskiej (ENISA). Mimo rosnącej skali zagrożeń cybernetycznych, skuteczna ochrona danych jest prostsza niż się wydaje – wystarczy kierować się kilkoma podstawowymi zasadami.

Duże koszty ataków hakerskich na placówki medyczne

Małe placówki medyczne coraz częściej padają ofiarą masowych ataków typu phishing oraz złośliwego oprogramowania. Wystarczy przez nieuwagę kliknąć w załącznik albo e-mail, a wirus blokuje dostęp do danych, np. kartotek pacjentów, i wykrada je.

***Phishing** często rozprzestrzenia się jako spam i dociera do niezliczonych odbiorców. To sposób na wykradanie danych do konta bankowego, maila, kart kredytowych czy informacji wrażliwych. Oszuści tworzą sposoby na to, aby „nabrać” użytkownika internetu, by kliknął w link czy skorzystał z zainfekowanej strony, która łudzaco przypomina konkretną witrynę, na przykład banku. Phishing wykorzystuje więc maile, wiadomości SMS, ale też portale społecznościowe czy sprzedażowe, poprzez które oszuści przesyłają linki do fałszywych stron internetowych. Często metodą jest podszywanie się w mailach pod różne osoby, firmy telekomunikacyjne, banki.*

Tego typu incydenty nie trafiają na czołówki gazet, ale mogą mieć poważne konsekwencje: problemy z ciągłością leczenia pacjentów, zakłócenia działalności placówki medycznej (łącznie z koniecznością jej zamknięcia na kilka dni), wysokie koszty pomocy udzielanej przez informatyków, bezpowrotną utratę danych. Nie wspominając o niebezpieczeństwie podjęcia błędnej decyzji medycznej w wyniku niekompletnych danych i karach finansowych, np. nakładanych przez Urząd Ochrony Danych Osobowych.

Udany atak hakerski wiąże się ze stresem, powoduje stratę czasu i pieniędzy. UODO co jakiś czas nakłada kary na placówki medyczne w efekcie nienależytej staranności w zakresie ochrony danych. Przykładem jest sprawa z sierpnia 2024 r., gdy UODO ukarał Spółkę American Heart of Poland SA, ponieważ źle szacowała ryzyko wycieku danych i nie przestrzegała własnej polityki ich bezpieczeństwa. W efekcie hakerzy uzyskali dostęp do danych osobowych około 21 tys. osób. Również w sierpniu tego roku prezes UODO nałożył karę 40 tys. zł na Samodzielny Publiczny ZOZ w Pajęcznie. W wyniku ataku hakerskiego placówka straciła dostęp do danych pacjentów i pracowników, a działania naprawcze podjęła dopiero po fakcie.

Wielowarstwowa ochrona danych

Najlepszą metodą ochrony danych jest tzw. model sera szwajcarskiego. Zakłada on, że nie ma jednego sposobu zapewniającego 100-proc. ochronę przed cyber-atakami. Ale im więcej warstw zabezpieczeń, tym większa szczelność systemu. Składają się na niego następujące elementy:

- **technologia:** aktualne systemy operacyjne i antywirusowe, automatyczne tworzenie kopii zapasowych (najlepiej w chmurze), systemy antywirusowe, mocne hasła dostępu, wirtualne sieci prywatne VPN (w przypadku pracy mobilnej);
- **ludzie:** wiedza na temat zagrożeń i ochrony przed nimi, czyli np. umiejętność rozpoznania wiadomości typu phishing, znajomość procedur w przypadku ataku cybernetycznego;
- **procedury:** opracowanie polityki ochrony danych zgodnej z RODO, plany postępowania. Każda placówka musi przeprowadzić weryfikację gromadzonych i przetwarzanych danych. Ogromną pomocą jest zatwierdzony przez UODO „Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych” opracowany przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie.

Od czego zacząć?

Personel medyczny nie musi być biegły w dziedzinie informatyki i poświęcać długich godzin na zapewnienie bezpieczeństwa danych, aby dobrze chronić się przed hakerami. Wystarczy kilka podstawowych zasad:

- wdrożenie reguł RODO, zgodnie z kodeksem Porozumienia Zielonogórskiego,
- inny komputer do pracy, a inny do spraw prywatnych,
- aktualny system operacyjny, czyli Windows 11,
- na bieżąco aktualizowany system gabinetowy,
- program antywirusowy,
- mocne i systematycznie zmieniane hasło,
- podwójna autentyfikacja do krytycznych danych,
- kopia zapasowa bazy danych w chmurze.

Poziom ochrony danych automatycznie się podniesie, gdy komputer albo laptop z systemem gabinetowym wykorzystywany będzie tylko do celów służbowych. Znaczna część ataków ransomware zaczyna się od kliknięcia w link w zainfekowanej wiadomości e-mail albo na stronie internetowej. Brak dostępu do e-maili automatycznie likwiduje to zagrożenie.

Komputer musi być wyposażony w aktualny system operacyjny, czyli Windows 11. Pamiętajmy, że od października 2025 r. Windows 10 przestanie być serwisowany i korzystanie z niego będzie oznaczać wystawianie się na ataki hakerów. Windows 11 daje silną ochronę, bo ma wbudowane dobre rozwiązanie antywirusowe Microsoft Defender. Mimo to, przyda się

dodatkowy program antywirusowy. Płatne wersje kosztują zazwyczaj 100–150 zł rocznie na jeden komputer, ale dodatkowo ułatwiają systematyczną konserwację komputera albo uruchomienie sieci prywatnej VPN, która jest wskazana przy pracy mobilnej.

Aktualne powinno być też oprogramowanie gabinetowe. Aby spać spokojnie, najlepiej skorzystać z opcji automatycznego tworzenia kopii zapasowej danych (backup) w chmurze. Taką opcję oferują dobrzy dostawcy IT. Nawet jeśli hakerzy zablokują komputer albo ulegnie on awarii, można będzie kontynuować pracę na innym urządzeniu i to bez utraty danych. Zdecydowanie bardziej opłaca się zainwestować w backup w chmurze, niż np. kupować drogie ubezpieczenie od zdarzeń cybernetycznych.

Nie zapominajmy również o systematycznej zmianie hasła. Jest to uciążliwe, ale mocne hasło stanowi jedno z najlepszych zabezpieczeń przed kradzieżą danych.

Co zrobić, gdy już dojdzie do ataku?

Dobre zabezpieczenia znacznie minimalizują ryzyko udanego ataku hakerskiego, nie chronią przed nim jednak w 100 proc. Pierwszą czynnością w przypadku ataku hakerów jest pilny kontakt telefoniczny z zespołem CSIRT Centrum e-Zdrowia (e-mail: csirt@cez.gov.pl) w celu uzyskania szybkiego wsparcia w formie zdalnej konsultacji.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa nakłada obowiązek formalnego zgłoszenia incydentu do UODO (zgłoszenie nie musi zawierać wszystkich informacji, można je uzupełniać na bieżąco). Wiele osób boi się, że dokonując zgłoszenia, naraża się na karę, gdy zostaną stwierdzone niedociągnięcia w ochronie danych. Warto jednak pamiętać, że większość kar wynika z zaniechania lub opóźnionego zgłoszenia. Dobra współpraca z UODO zwiększa prawdopodobieństwo, że sprawa zakończy się upomnieniem, a nie karą finansową.

Pod żadnym pozorem nie należy próbować płacić okupu. Powód jest pragmatyczny: nawet po wpłacie nie ma gwarancji, że hakerzy odblokują dostęp do komputera. Warto też mieć sprawdzonego informatyka, który pomoże przywrócić pracę komputera i odzyskać dane.