Szpitale to dla hakerów kopalnie złota

O cyberbezpieczeństwie „Panaceum” rozmawia z Piotrem Kalkowskim, pełnomocnikiem ds. rozwoju informatyzacji Naczelnej Izby Lekarskiej.

„Panaceum”: – Śledząc doniesienia medialne, łatwo zauważyć, że ataki hakerskie na szpitale i duże ośrodki zdrowia, stają się coraz częstsze. Zastanawiam się, dlaczego tak się dzieje i czego hakerzy mogą tam szukać. Czy chodzi o bazy danych?

Piotr Kalkowski: – W dyskusji o cyberbezpieczeństwie najważniejsze jest ustalenie, jakie zasoby mogą być dla drugiej strony na tyle wartościowe, by dokonała ona złamania prawa. Szpitale to istne kopalnie złota, mamy tu bazy bardzo wrażliwych danych i to zarówno danych pacjentów, jak i lekarzy. To informacje, które mogą posłużyć do bardzo wielu celów, nawet do szantażowania osób, których dotyczą. Przecież informacje medyczne to jedne z najtajniejszych danych w naszym prywatnym życiu. Hakerzy mogą też dokonać odwróconej próby uzyskania dostępu. Ktoś może chcieć wprowadzić do systemu dodatkowe informacje, które mogą być wykorzystane na przykład przy próbach wyłudzenia odszkodowań. Słowem, szpital to skarbnica najważniejszych informacji, które chcemy chronić.

Tu natychmiast pojawia się wniosek, że te dane powinny być szczególnie chronione. Czy tak jest w istocie?

Cyberbezpieczeństwo kosztuje i wymaga świadomości użytkowników. W obie te rzeczy trzeba inwestować, zarówno czas, jak i zasoby ludzkie.

Czy najsłabszym ogniwem są ludzie?

Najczęściej. Pracownik szpitala – lekarz czy pracownik administracyjny powinien być przeszkolony w kwestii cyberbezpieczeństwa i przede wszystkim zdawać sobie sprawę z zagrożeń. Tymczasem wszyscy wiemy, jak to wygląda w szpitalach. Zdajemy sobie sprawę, że niejednokrotnie podrzucaliśmy kartę ze swoim numerem identyfikacyjnym koledze, żeby mógł szybciej się zalogować. Jak zostawialiśmy ją przy komputerze. Ile razy widzieliśmy jak koleżanka umieszcza hasło do komputera na monitorze, tak że może być widoczne nie tylko dla innych pracowników, ale nawet dla ludzi z zewnątrz. To są codzienne zachowania, które są potencjalnie bardzo niebezpieczne. To właśnie takie,

na pozór drobne błędy, mogą pokonać nawet najlepszy system informatyczny.

Czy jest na to sposób?

Można chronić się na dwa sposoby. Po pierwsze, ograniczając dostęp pojedynczego pracownika do systemu, chociaż w szpitalach bywa to trudne. Lekarze muszą mieć dostęp do różnych danych, na dodatek często liczy się czas. Po drugie, szkolenie, szkolenie i jeszcze raz szkolenie. Pracownicy muszą wiedzieć, co robią nie tak i jakie ryzyko niosą za sobą pozornie tylko błahe zaniedbania. Dobrym rozwiązaniem jest przeprowadzenie audytu, który wykaże między innymi, gdzie pracownicy popełniają błędy. Nie po to, by ich karać, ale żeby pokazać, czym może to grozić.

Domyślam się, że działania związane z zapewnieniem cyberbezpieczeństwa nie są tanie.

Nie są i to z dwóch powodów. Po pierwsze sama infrastruktura zabezpieczająca przed atakami hakerskimi kosztuje. To kwestia sprzętu i licencji. Po drugie to koszty osobowe. Na rynku komercyjnym koszt pracy specjalisty w tej dziedzinie to wydatek rzędu 200–300 zł za godzinę.

Szpitale na co dzień stają przed dylematem „na co tym razem zabraknie pieniędzy". Nic dziwnego, że kwestie informatyczne schodzą na drugi plan.

To wynika raczej z całkowitego zaniedbania tej kwestii. Z kompletnego braku świadomości o jakie zagrożenie chodzi. Szpitale dysponują często nowoczesnym sprzętem kupionym za środki unijne, co z tego, jeśli nie jest on odpowiednio skonfigurowany?

Przecież podczas ataku hakerskiego zagrożone są nie tylko dane, może być także zagrożone zdrowie i życie pacjentów.

Najgłośniejsze ataki, do których dochodzi na świecie, dotyczą żądań okupu. Wirus dostaje się do systemu i szyfruje wszystkie dane znajdujące się na dyskach, w tym dokumentację medyczną. Nie trudno sobie wyobrazić, do czego może doprowadzić taka sytuacja.

Jak się przed tym zabezpieczyć? Czy to w ogóle możliwe?

Wracamy do projektowania systemu. To na tym etapie musimy przewidzieć, że pewna część systemu może zostać przejęta i że poszczególne jego moduły powinny móc działać niezależnie. Nigdy całkowicie nie zapobiegniemy atakom, ale możemy znacznie zminimalizować ewentualne straty.

Co pańskim zdaniem jest największym problemem w dziedzinie

cyberbezpieczeństwa: braki sprzętu, jego niewłaściwe użytkowanie, czy brak przeszkolenia personelu?

Myślę, że największym problemem jest brak świadomości osób zarządzających szpitalami.

Co więc możemy podpowiedzieć zarządzającym?

Przede wszystkim należy przestać się bać audytu. Należy zlecić analizę systemu zewnętrznej firmie. Po uzyskaniu raportu wykazującego błędy, można je zacząć naprawiać. To znacznie mniejsze koszty niż nieuzasadniona rewolucja całego systemu.

Jak wygląda rynek usług w tym sektorze w Polsce. Czy istnieje wiele firm zajmujących się cyberbezpieczeństwem?

Jesteśmy rozwiniętym europejskim rynkiem i jeśli chodzi o komercyjne usługi dla firm, nie odstajemy od innych krajów. Ponadto polscy specjaliści są jednymi z najlepszych w Europie. Problem w tym, że cena zawsze będzie w euro...

A szpitale, jak wiadomo, cierpią na wieczny brak środków.

Środków można szukać na zewnątrz. Narodowy Fundusz Zdrowia dysponuje budżetem, który można pozyskać w celu przeprowadzenia audytu. To tylko jedna z możliwości. Najważniejsze, żeby zdać sobie sprawę z zagrożenia, które z dnia na dzień staje się coraz bardziej realne.

Rozmawiała Justyna Kowalewska

Panaceum 4/2023