**Hakerzy atakują „na telemedycynę”**

* **Liczba cyberataków na służbę zdrowia i pacjentów wzrosła o 55% - co tydzień dochodzi średnio do 752 prób naruszenia systemów medycznych.**
* **Przychodnie, szpitale, a także dostawcy innych usług powinni zadbać przede wszystkim o poufność i dostępność swoich systemów, jak i ich integralność, żeby uniknąć luk.**
* **Podstawą skutecznej obrony są regularne testy zabezpieczeń, włącznie z symulowaniem ataków.**

Rosnące zagrożenie atakami hakerskimi obserwujemy już od wielu lat, ale ostatnie kilkanaście miesięcy to swoisty „rozkwit” działalności cyberprzestępców. Według danych gromadzonych przez Check Point liczba ataków na służbę zdrowia wzrosła we wrześniu o 55%, porównując rok do roku. W liczbach bezwzględnych oznacza to, że co tydzień przestępcy atakują sektor zdrowia średnio 752 razy.

Jedną z przyczyn jest wymuszona przez pandemię i lockdowny przyspieszona cyfryzacja wielu sfer naszego życia. A przestępcy wykorzystują każdą okazję i ostatnimi czasy coraz częściej atakują właśnie służbę zdrowia i pacjentów, co może być szczególnie groźne. Przykładowo, w lipcu hakerzy zablokowali dostęp do danych klinicznych szpitala w Bukareszcie, w sierpniu zdezorganizowali na kilka godzin szczepienia przeciw COVID-19 we włoskim regionie Lacjum, a wiosną zaatakowali ransomware publiczną służbę zdrowia w Irlandii, przez co odwołano część zaplanowanych porad lekarskich. Te zdarzenia mogą mieć tragiczny finał, jak atak na centrum kliniczne w Duesseldorfie w zeszłym roku, który doprowadził do śmierci pacjentki, ponieważ wskutek blokady systemów nie otrzymała na czas pomocy.

– *Spadku liczby i częstotliwości cyberataków na szpitale, przychodnie czy firmy zajmujące się ochroną zdrowia, nie należy się spodziewać. Zwłaszcza że współczesne technologie pozwalają przestępcom w szybki i prosty sposób podszyć się np. pod pracownika rejestracji POZ i wyłudzić od nas wrażliwe informacje lub pod przedstawiciela NFZ, żeby zaatakować placówkę medyczną. Tego typu ataki nasiliły się wraz z upowszechnieniem teleporad. Drugim powodem zainteresowania przestępców branżą zdrowotną jest fakt, że atakując „na telemedycynę” lub placówki medyczne, przestępcy otrzymują dostęp do wielu poufnych danych jednocześnie. Jedynym sposobem walki z hakerami jest regularne sprawdzanie i aktualizowanie zabezpieczeń oraz prowadzenie akcji informacyjnych wśród pracowników służby zdrowia i pacjentów, ponieważ to my, ludzie stanowimy najsłabsze ogniwo zabezpieczeń* – zauważa Michał Bukontt, Dyrektor Sprzedaży w Sprint S.A., ekspert ds. cyberbezpieczeństwa.

**Jak zabezpieczyć placówkę medyczną?**

Współczesne placówki medyczne korzystają z wielu różnych systemów i narzędzi IT. Dlatego dbając o ich bezpieczeństwo cybernetyczne, trzeba pamiętać przede wszystkim o trzech najważniejszych kwestiach, które warto poddawać regularnym testom:

* **Poufności** – pod tym pojęciem należy rozumieć bezpieczeństwo wszystkich systemów, baz i rejestrów gromadzących dane pacjentów pod kątem kontroli dostępu osób, procesów lub innych podmiotów, żeby uniknąć połączeń nieuprawnionych. Zadbać należy jednak nie tylko o same zbiory, dostęp do nich oraz sposób przetwarzania informacji, ale również o przestrzeganie odpowiednich procedur pozyskiwania tych wrażliwych danych. To ich kradzież jest najczęściej celem hakerów.
* **Integralności** – zabezpieczenie danych wprowadzeniem w nich zmian w nieautoryzowany sposób. W tym celu wszystkie systemy działające w placówce powinny być ze sobą spójne – to zapewnia ochronę przed zmianą w trakcie przesyłania oraz zabezpiecza przed zmianami przez nieupoważnione osoby lub procesy. Testować i monitorować warto przede wszystkim sposób wymiany danych wewnątrz organizacji, pomiędzy różnymi systemami. Tu najłatwiej o luki.
* **Dostępności** – rozumianej jako  zapewnienie dostępu do danych osobom uprawnionym w założonym czasie, czyli unikanie zablokowania dostępu. Szczególnie dotkliwe w skutkach mogą tu być np. podatność na ataki ransomware czy popularne w przypadku stron internetowych, ataki bazujące na odmowie usługi (DoS, DDoS). Szczególnie narażone są serwisy, za których pośrednictwem można np. pobrać wyniki badań – to wręcz wymarzony cel dla hakerów.

– *Niepokojącym faktem jest również to, że naruszenie bezpieczeństwa systemu, szczególnie gdy przestępcy chcą pozyskać dane osobowe, wykrywane jest zazwyczaj dopiero po wielu miesiącach. Średnio po ponad 200 dniach. Dlaczego tak się dzieje? Haker po uzyskaniu dostępu najczęściej nie „rzuca się” od razu na dane. Po złamaniu zabezpieczeń zmniejsza swoją aktywność i dopiero po jakimś czasie zaczyna po kolei wykradać poszczególne informacje, sprawdzając jednocześnie, jak skuteczne są nasze zabezpieczenia. Jak już przekona się, na co może sobie pozwolić, przypuszcza właściwy atak. Dlatego tak ważne jest regularne testowanie infrastruktury IT i symulowania ataków, zarówno własnymi siłami, jak i z pomocą zewnętrznych ekspertów* – dodaje Michał Bukontt ze Sprint S.A.

**3 podstawy audytów IT**

Skuteczny audyt IT powinien składać się z kilku etapów. Warto przeprowadzić zarówno testy zewnętrzne, jak i wewnętrzne. Pierwsze sprawdzają zdolność obrony przed uzyskaniem dostępu bezpośrednio z Internetu. Drugie, jak nazwa wskazuje, służą wykryciu luk wewnątrz naszych systemów – nieprawidłowości w konfiguracji urządzeń, sieci. Trzecim aspektem, który też należy testować, są zachowania pracowników – przestrzeganie procedur, czujność wobec podejrzanych zdarzeń oraz sposób reagowania, gdy dojdzie do błędu. To obecnie podstawowe działania, które warto regularnie prowadzić.

Źródło: Sprint S.A.