**Cyberepidemia w służbie zdrowia**

**Służba zdrowia w ostatnim czasie była celem wielu poważnych cyberataków. W ciągu dwóch ostatnich lat nastąpiło tysiące włamań, podczas których wykradziono osobiste dane medyczne (PHI – personal health information) milionów pacjentów. Według Centrum Kradzieży Tożsamości (Identity Theft Resource Center), 42.5 procenta wszystkich włamań nastąpiło w sektorze opieki zdrowotnej. Centrum informuje także, że 91 procent firm związanych ze służbą zdrowia padło ofiarą przynajmniej jednego włamania w ciągu ostatnich dwóch lat.[1]**

W Stanach Zjednoczonych, gdzie pomimo regulacji HIPAA (Health Insurance Portability and Accountability Act), które wprowadzają obowiązek ochrony prywatnych danych pacjentów, wiele badań wskazuje na nagły wzrost przypadków kradzieży danych.

*W jednym z raportów opublikowanych w Journal of American Medical Association przeanalizowano bazę danych Ministerstwa Zdrowia i Opieki Społecznej zawierającą ujawnione przez HIPAA wycieki danych z ponad 500 firm w latach 2010-2013. Artykuł wskazuje, że w tym okresie miało miejsce 949 włamań dotyczących w sumie 29 milionów rekordów. Sytuacja pogarsza się z roku na rok. W bieżącym roku firma Anthem ogłosiła, że doszło do włamania, które dotknęło około 80 milionów ludzi* – twierdzi Jessica Cooper z firmy Check Point.

A to tylko wierzchołek góry lodowej. Po głośnym ataku na Anthem, doszło do wycieków danych w CareFirst BlueCross BlueShield oraz Premera BlueCross BlueShield. Oba włamania znalazły się wśród 10 największych w bieżącym roku… [[2]](http://blog.checkpoint.com/2015/10/19/our-mission-to-cure-the-healthcare-security-epidemic/#_ftn3)

***Dlaczego hakerzy obierają sobie za cel służbę zdrowia?***

Przede wszystkim dane medyczne stają się celem ataków, gdyż są one bardzo cenne. Ich wartość wynika z tego, że zawierają kompletne dane o stanie zdrowia (PHI), informacje identyfikacyjne (takie jak data urodzenia czy numery ubezpieczeń społecznych), a mogą również zawierać dane finansowe/dane kart kredytowych. Wszystko to może zostać użyte do kradzieży tożsamości i może zrujnować finansowo ofiary ataków.

Po drugie, wielkim wyzwaniem dla organizacji jest opóźnienie we wprowadzaniu najnowszych technologii. Środowiska firm medycznych mają bardzo wymagającą strukturę IT oraz sieci, których granica nie jest jasno zdefiniowana. Zagrożenia stają się bardziej inteligentne z dnia na dzień, więc dyrektorzy działów IT powinni określić strategie bezpieczeństwa, aby ochronić swoje firmy przed stale zmieniającymi się zagrożeniami. Nasza rosnąca zależność od podłączonych urządzeń medycznych stanowi dodatkowy wektor ataku. Z tych powodów, firmy medyczne są głównymi celami cyberprzestępców.

Służba zdrowia to bardzo złożony, wielopoziomowy ekosystem, który wymaga zaawansowanej ochrony przed zaawansowanymi cyberzagrożeniami. To oznacza, że potrzeba zintegrowanych rozwiązań, które ochronią przed atakami typu persistent threat oraz zero-day, a także pomogą organizacjom sprostać regulacjom HIPAA oraz PCI DSS, jednocześnie umożliwiając pełen wgląd w swoje operacje dla scentralizowanego systemu zarządzania bezpieczeństwem.

*Istnieje szereg punktowych zabezpieczeń dostępnych na rynku. Niestety większość z tych produktów nastawiona jest na reagowanie na konkretne zagrożenia, a nie całościową ochronę. Wierzymy, że firmy potrzebują scentralizowanego, zintegrowanego podejścia do tematu cyberbezpieczeństwa* – dodaje Cooper.

W jaki sposób to osiągnąć? Przede wszystkim zrozumieć potrzebę ochrony wykraczającej poza standardowe oprogramowanie antywirusowe oraz spełniającej wszelkie regulacje. Dzisiejsze firmy medyczne potrzebują jednego rozwiązania, które łączy urządzenia bezpieczeństwa sieci o wysokiej efektywności oraz aktywną ochronę czasu rzeczywistego. Potrzeba wysoce inteligentnej technologii, która nadąża za zmieniającymi się zagrożeniami – technologii, która potrafi wykryć i zablokować zarówno znane jak i nieznane zagrożenia, a także spełniać wytyczne regulacji prawnych oraz dać Ci pełen wgląd w stan bezpieczeństwa firmy.