PESEL z przychodni gratką dla hakera

Kategoria: Styl życia
Opublikowano: środa, 22, listopad 2023 08:45
Joanna Gryboś-Chechelska

Placówki medyczne to skarbnice danych osobowych i wrażliwych. Dla hakerów to źródło niewyobrażalnych wręcz zysków, zwłaszcza że dostęp do nich nie jest zbyt trudny. Z powodu chronicznego niedoinwestowania poziom zabezpieczeń jest bardzo niski, do tego dochodzą luki w oprogramowaniu czy nieprzestrzeganie procedur przez ludzi. Według danych Ministerstwa Cyfryzacji liczba zgłoszonych cyberataków na placówki ochrony zdrowia w Polsce wzrosła trzykrotnie w ciągu roku i nadal rośnie. A to tylko wierzchołek góry lodowej, bo o wielu skutecznie przeprowadzonych włamaniach nie wiemy.

Przed pandemią w szpitalach rocznie leczyło się ok. 8 mln pacjentów rocznie. Placówki te gromadziły dane nie tylko o leczonych tu chorobach, ale też te, które identyfikowały pacjenta – imię i nazwisko, PESEL, adres zamieszkania. Przez Covid liczba hospitalizacji zmalała do ok. 5,7 mln, nadal to jednak olbrzymi zbiór danych osobowych. Znacznie więcej jest ich jednak w przychodniach. Niezależnie od tego czy ktoś choruje, czy nie, jego dane osobowe są albo w przychodni publicznej albo i publicznej i prywatnej. A poziom zabezpieczenia wszystkich nie należy do najwyższych.

Tymczasem służba zdrowia stała się głównym celem cyberataków, zarówno w Polsce, jak i na świecie. W Polsce liczba zgłoszonych cyberataków na placówki ochrony zdrowia wzrosła trzykrotnie w ciągu jednego roku – z 13 w 2021 do 43 w 2022, co wynika z oficjalnych danych Ministerstwa Cyfryzacji. Na świecie opieka zdrowotna jest najczęściej atakowanym sektorem z blisko 1800 atakami tygodniowo, a w 2022 roku branża zanotowała wzrost liczby ataków o 74 proc. – ujawniają eksperci firmy Check Point Research.

– Są różne rodzaje ataków hakerskich. Te, o których słyszymy i które pojawiają się w oficjalnych statystykach, to najczęściej ataki typu ransomware czy DDos. Pierwszy polega na zainfekowaniu systemu informatycznego złośliwym oprogramowaniem, które szyfruje dane użytkownika uniemożliwiając korzystanie z nich. Drugi to wysyłanie wielu zapytań przez zainfekowane komputery, które powodują przeciążenie serwera atakowanej placówki paraliżując jej system komputerowy. A ich celem jest wymuszenie okupu. Takie ataki są widoczne, dlatego o nich słyszymy, widzimy je w statystykach. Ale jak hakerzy wykradną dane pacjentów, to często dowiemy się o tym dopiero wtedy, kiedy zacznie się do nich zgłaszać komornik za niespłacanie kredytów, które ktoś zaciągnął na ich konto – tłumaczy Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Do najgłośniejszego ataku ransomware na placówkę medyczną doszło rok temu – wówczas ofiarą hakerów padło Centrum Zdrowia Matki Polki. Kilka miesięcy później podobny atak na Centralny Szpital Kliniczny w Łodzi się nie powiódł – podejrzane działania zostały zauważone i specjaliści od cyberbezpieczeństwa profilaktycznie wyłączyli systemy informatyczne szpitala. Dlatego przestępcy nie poprzestają tylko na atakowaniu dużych placówek, które zaczynają być lepiej chronione. Wybierają na ofiarę mniejsze ośrodki, tak było w przypadku szpitala w Pajęcznie.

Naruszenia w sektorze medycznym, związane z tzw. przełamaniem zabezpieczeń czy też atakiem ransomware są regularnie zgłaszane Prezesowi UODO.

– Nie są one tak liczne jak naruszenia powstałe w wyniku tzw. ludzkiego błędu. Jednak z uwagi na swój charakter, a w szczególności na liczbę osób oraz kategorie danych objętych incydentem, generują co do zasady wysokie ryzyka dla praw lub wolności osób fizycznych. Biorąc pod uwagę, że służba zdrowia przetwarza olbrzymią ilość tzw. szczególnych kategorii danych osobowych, które można bez przesady określić jako „dane krytyczne dla funkcjonowania społeczeństwa" oraz fakt, iż systemy informatyczne w

określonych placówkach zdrowia nadal nie spełniają wymogów zgodnych z ogólnym rozporządzeniem o ochronie danych (RODO), nie dziwi fakt, że liczba ataków nie maleje, a biorąc pod uwagę zapowiedzi kolejnych działań mających na celu digitalizację usług medycznych, zapewne będzie wzrastać w kolejnych latach – mówi Adam Sanocki, rzecznik prasowy Urzędu Ochrony Danych Osobowych.

Skala zagrożenia związanego z atakami na infrastrukturę IT w służbie zdrowia jest tak duża, że Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), niezależna agencja Unii Europejskiej, postanowiła przyjrzeć się temu problemowi. Unijni eksperci przeanalizowali wszystkie incydenty cybernetyczne, zgłoszone w krajach UE od stycznia 2021 roku do marca 2023 roku. Na tej podstawie powstał raport "Health Threat Landscape". Wynika z niego, że ransomware to jedno z głównych zagrożeń w sektorze zdrowia, stanowiąc 54 proc. wszystkich incydentów. Co więcej, 43 proc. incydentów związanych z ransomware wiązało się z naruszeniem danych lub kradzieżą danych. To podkreśla fakt, że nawet w przypadku ataków mających na celu wyłudzenie okupu, dane pacjentów są również celem hakerów. Dane pacjentów były najczęściej atakowanym aktywem, stanowiąc 30 proc. wszystkich incydentów.

– Należy również zwrócić uwagę, iż ataki hakerskie nie koncentrują się wyłącznie na dużych podmiotach medycznych – w ich przypadkach skuteczny atak może wymagać niekiedy dużego nakładu pracy z uwagi na wdrożone środki bezpieczeństwa – ale również na małych podmiotach, prowadzonych często przez osoby fizyczne, które nie wdrożyły na czas adekwatnych środków w celu ochrony swoich zasobów – wskazuje Adam Sanocki z UODO.

Eksperci od cyberbezpieczeństwa podkreślają, że mała liczba ujawnionych przypadków kradzieży danych osobowych z placówek medycznych w Polsce nie powinna nas uspokajać. Jeśli w znacznie bogatszych i bardziej zaawansowanych technologicznie krajach Europy Zachodniej, Stanach Zjednoczonych czy Kanadzie odnotowuje się rosnącą liczbę skutecznych ataków na bazy danych placówek medycznych, to trudno się spodziewać że w Polsce takie zjawisko nie występuje. Raczej należy przyjąć założenie, że nie potrafimy go wykryć.

– Podobnego zdania są Polacy. Z przeprowadzonego w kwietniu 2023 roku przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych badania „Dane osobowe – czy wiemy, jak je chronić?" wynika, że wyciek danych z instytucji publicznych i firm prywatnych jest drugim pod względem liczby wskazań zagrożeniem dla danych osobowych identyfikowanym przez dorosłych Polaków. Obawy takie wyrażało 38 procent respondentów. Większe zagrożenie dla bezpieczeństwa danych osobowych widzieli tylko w fałszywych SMS-ach, e-mailach i telefonach – co stanowiło 42 procent wskazań – komentuje Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Źródło: IP