PROTOKÓŁ z XX posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 8 listopada 2024 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

Otwarcie posiedzenia – Pani Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Pani Przewodnicząca powitała obecnych członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości.

Cyberbezpieczeństwo w sektorze zdrowia:

1. Zagrożenia dla systemów e-zdrowia w świetle obserwowanych przez CERT Polska incydentów - Pan Sebastian Kondraszuk, Kierownik Działu CERT Polska w Naukowej i Akademickiej Sieci Komputerowej.

Pani Agnieszka Gryszczyńska zaznaczyła, że posiedzenie poświęcone tematyce cyberbezpieczeństwa w sektorze zdrowia ma na celu ukazanie problemów, które w części można rozwiązać lub zaproponować rozwiązania do wprowadzenia w dalszej perspektywie. Inspiracją do podjęcia tematu są postępowania prowadzone przez prokuraturę z zakresu zróżnicowanych metod eksploracji danych pacjentów, lekarzy i wykorzystania tych danych na wystawianie recept głównie na leki opioidalne, co nie jest jednak jedynym celem, dla jakiego dane są pobierane. Pani A. Gryszczyńska zapowiedziała przedstawienie działań podejmowanych przez poszczególne służby organów ścigania. Pewne rekomendacje zostały już wdrożone w instytucjach sektora zdrowia, jednak wydaje się, że bez zmian legislacyjnych nie ma możliwości zwiększenia cyberbezpieczeństwa danych nas wszystkich, a także bezpieczeństwa systemu e-zdrowia. Po krótkim wprowadzeniu Pani A. Gryszczyńska oddała głos Panu S. Kondraszukowi.

Pan Kondraszuk nakreślił aspekty, które są słabością nie tylko użytkowników systemu zdrowia, ale także użytkowników szeroko rozumianych systemów teleinformatycznych, co przekłada się na dużą liczbę incydentów związanych z wyprowadzaniem różnego rodzaju danych. Zaznaczył, że obszar operowania CERT Polska jest najszerszy spośród CSIRTów poziomu krajowego. Skupiając się na samej służbie zdrowia jako sektorze, za cyberbezpieczeństwo którego CERT Polska także w części odpowiada, jest to obszar najszerszy w myśl Dyrektywy NIS 1, gdzie znajduje się blisko 300 operatorów usług kluczowych. Implementacja Dyrektywy NIS 2 spowoduje, że zakres podmiotów, które będą musiały dostosowywać się do nowych regulacji zostanie poszerzony. Pan Kondraszuk przedstawił kanał zgłoszeniowy CERT Polska, który jest motorem napędowym bardzo dużej części pracy CERT Polska. Prowadzone są także samodzielne metody identyfikacji zagrożeń i incydentów. Wskazana została liczba zgłoszeń skierowanych w obecnym roku do CSIRTu NASK oraz liczba zarejestrowanych incydentów. Zauważone zostało, że począwszy od roku 2020 nastąpił dynamiczny przyrost rejestrowanych incydentów powiązanych z jedną specyficzną kategorią - oszustw internetowych. Za warte odnotowania uznano, iż incydenty dla sektora zdrowia stanowiły zaledwie 0,5% incydentów obsłużonych przez CERT Polska,

mając jednak na uwadze skutek tych incydentów były one bardzo znaczące. Oszustwa komputerowe stanowią blisko 95% incydentów obsługiwanych przez zespół CERT Polska. Wskazano na działania podejmowane przez CERT Polska, zarówno o charakterze operacyjnym, koordynacyjnym jak również legislacyjnym (w tym uczestnictwie w przygotowaniu regulacji odnoszącej się do zwalczania nadużyć w komunikacji elektronicznej[1]). Zauważone zostało, że w kategorii oszustw komputerowych zawiera się kategoria phishingu, z którym CERT Polska walczy od 30 lat. Za sukces uznano listę ostrzeżeń przed domenami wyłudzającymi dane funkcjonującą od 2020 r. Przedstawiciel NASK wskazał, że operatorzy CERT Polska w trybie ciągłym klasyfikują domeny. Lista domen jest dostępna w postaci wykazu, który można zaimplementować w dowolnym miejscu. Podejmowane są starania, aby lista została zaimplementowana jak najszerzej, także w mniejszych podmiotach.

Pan S. Kondraszuk przedstawił przykłady podszywania się pod różnego rodzaju podmioty z sektora zdrowia. Wspomniał także o różnego rodzaju podatnościach, w tym w aplikacjach i systemach wykorzystywanych w sektorze zdrowia. Zaznaczył, że prowadzone są proaktywne skanowania podmiotów w sektorze służby zdrowia. Wskazał, że ograniczenie skutków ataków na użytkowników służby zdrowia ma dla CERT Polska wysoki priorytet, ze względu na obsługiwanie wyjątkowo wrażliwych danych.

2. Aktualne metody eksploracji przez cyberprzestępców danych i systemów e-zdrowia- Pani Agnieszka Gryszczyńska, RdC oraz Pan Dariusz Śpicha, Naczelnik Wydziału Operacyjno-Śledczego Zarządu Centralnego Biura Zwalczania Cyberprzestępczości w Krakowie.

Pan Naczelnik na wstępie wskazał, że CBZC zajmuje się cyberprzestępczością - nie cyberbezpieczeństwem. Przedstawił wektory ataków na usługi e-zdrowia oraz ich ewolucję od czasu rozpoczęcia pandemii, pojawienia się szczepionki przeciw COVID – 19 i możliwości elektronicznej rejestracji w systemach zdrowia. Pan Naczelnik omówił sposoby działania cyberprzestępców, uzyskane korzyści oraz aspekty wykorzystania danych i systemów, których gestorami są różne podmioty.

Rozpoczęła się dyskusja na temat przepływu informacji między podmiotami z sektora zdrowia. Zastanawiano się jaką rolę może pełnić Rada w przedmiotowym temacie. Wyrażono zdanie, że należy rozdzielić dwie sprawy - odpowiedzialność określonych podmiotów oraz wsparcie CSIRTów. Poruszona została kwestia uprawnień organu nadzorującego oraz zmian w ustawie o krajowym systemie cyberbezpieczeństwa[2]. Pani A. Gryszczyńska wspomniała, że zostały stworzone rekomendacje poszczególnych podmiotów w zakresie zmian w przepisach. Wyraziła jednak nadzieję na wypracowanie rekomendacji z punktu widzenia członków Rady. Uznano, że należy dążyć do sporządzenia stanowiska, które będzie skierowane nie tylko do Ministra Cyfryzacji, ale także do Ministra Zdrowia, bowiem bez zmian przepisów sytuacja walki z cyberprzestępczością nie ulegnie poprawie. Wyrażone zostało zdanie, by stworzyć

[1] Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. 2023 poz. 1703)
[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077)

twarde minimalne obowiązki, zasady odpowiedzialności określonych podmiotów i wymagania bezpieczeństwa dla aplikacji gabinetowych.

3. Wnioski Zakładu Ubezpieczeń Społecznych płynące z obserwacji aktualnych incydentów- Pan Sławomir Wasielewski, Członek Zarządu nadzorujący Pion Operacji i Eksploatacji Systemów w ZUS; Pani Agnieszka Gębicka, Dyrektor Biura Ochrony Danych Osobowych w ZUS; Pan Tomasz Sadowski, Dyrektor Departamentu Cyberbezpieczeństwa w ZUS.

Pan S. Wasielewski na początku wypowiedzi wspomniał o wdrożeniu dwuskładnikowego uwierzytelniania w systemie PUE ZUS oraz o wdrożeniu e-zwolnień w ramach PUE. ZUS zdecydował, aby we współpracy z Naczelną Izbą Lekarską wypracować rozwiązanie przyjazne dla lekarzy - podpisywanie zwolnień wyłącznie drogą elektroniczną. Po wprowadzeniu kolejnych przepisów oraz zmian, certyfikat dla lekarzy zaczął być wykorzystywany do innych działań. Wskazano i wymieniono grupy uprawnionych (głównie do wystawiania e-recept). ZUS poddaje pod zastanowienie czy w związku z tym, że certyfikat nie odpowiada dzisiejszym wyzwaniom należy stworzyć jedno rozwiązanie dla wszystkich lekarzy do wszelkich zastosowań. Jeśli jednak ZUS miałby podwyższać poziom bezpieczeństwa certyfikatu i jego wydawania, to pojawia się pytanie czy warto przeprowadzić działania w tym kierunku, czy skorzystać z gotowych rozwiązań oraz w jaki sposób przedsięwzięcie powinno być współfinansowane, mając na uwadze, że certyfikat jest wykorzystywany do większości zadań niezwiązanych ze statutową działalnością ZUS.

Pani Dyrektor A. Gębicka dodała, że nowelizacja ustawy o systemie ubezpieczeń społecznych[3] rozszerzyła wykorzystywanie certyfikatu na inną dokumentację medyczną oraz e-recepty.

4. Propozycje działań mających na celu zwiększenie bezpieczeństwa danych pacjentów wobec obserwowanych zagrożeń - Pan Tomasz Jeruzalski, Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych, Centrum e-Zdrowia; Pan Andrzej Sarnowski, Dyrektor Pionu Rozwoju SIM i Wdrożeń, CeZ; Pan Wojciech Demediuk, Dyrektor Departamentu e-Zdrowia w Ministerstwie Zdrowia.

Przedstawiciele Centrum e-Zdrowia przedstawili informacje dotyczące aplikacji gabinet.gov.pl oraz obszaru systemów gabinetowych. Rozróżniono te dwa systemy, a także miejsca występowania wektorów ataków, potencjalne działania oraz rekomendacje.

Omówiono proces wystawiania e-recept i wspomniano o przechowywaniu danych w systemach komercyjnych. Następnie, przedstawiono działania i procesy w aplikacji gabinet.gov.pl. Zauważono, że większość nadużyć dotyczy systemów komercyjnych. Zwrócono uwagę na zidentyfikowanie problemów kradzieży tożsamości. W dalszej części wypowiedzi podano liczbę uprawnionych do wystawiania recept. Przedstawiciele CeZ poinformowali, że w celu ograniczenia kwestii nadużyć związanych z ich wystawianiem, zostały wprowadzone limity ilościowe na wskazany czas.

[3] Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. 2024 poz. 497)

Zauważono że art. 8b ustawy o systemie informacji w ochronie zdrowia[4] przewiduje przepisy zobowiązujące usługodawców oraz podmioty prowadzące rejestry medyczne do zapewnienia zgodności swoich systemów teleinformatycznych z minimalnymi wymaganiami technicznymi i funkcjonalnymi zamieszczanymi w BIP ministra właściwego ds. zdrowia. W systemach usługodawców położony był dotychczas nacisk tylko na aspekty funkcjonalne. Zarekomendowano zaktualizowanie dokumentu poprzez dodanie wymagań z zakresu bezpieczeństwa.

5. Dyskusja.

W toku dyskusji zastanawiano się nad sposobem przeciwdziałania cyberprzestępczości w sektorze zdrowia. Uznano za konieczne prowadzenie działań legislacyjnych zmierzających do wdrożenia odpowiednich rozwiązań zgodnie z wypracowanymi rekomendacjami.

Pani Przewodnicząca poprosiła zaproszonych gości o przekazanie Radzie swoich rekomendacji. Zadecydowała, aby 22 listopada zainteresowani przedmiotowym tematem członkowie Rady, spotkali się w formie zdalnej w celu kontynuacji wątku cyberbezpieczeństwa w sektorze zdrowia i wypracowania stanowiska, które zostanie przekazane Panu Wicepremierowi Krzysztofowi Gawkowskiemu.

Zakończenie posiedzenia.

[4] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2023 poz. 2465)

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska – Przewodnicząca
6. Jolanta Jaworska
7. Michał Kanownik
8. Janusz Kosiński
9. Anna Beata Kwiatkowska
10. Jarosław Mojsiejuk
11. Patrycja Staniszewska
12. Katarzyna Szymielewicz
13. Robert Trętowski

Zaproszeni goście:

14. Dariusz Śpicha, Naczelnik Wydziału Operacyjno – Śledczego Zarządu Centralnego Biura Zwalczania Cyberprzestępczości w Krakowie
15. Sebastian Kondraszuk, Kierownik Działu CERT Polska w Naukowej i Akademickiej Sieci Komputerowej
16. Sławomir Wasielewski, Członek Zarządu nadzorujący Pion Operacji i Eksploatacji Systemów w Zakładzie Ubezpieczeń Społecznych
17. Agnieszka Gębicka, Dyrektor Biura Ochrony Danych Osobowych w Zakładzie Ubezpieczeń Społecznych
18. Tomasz Sadowski, Dyrektor Departamentu Cyberbezpieczeństwa w Zakładzie Ubezpieczeń Społecznych
19. Tomasz Jeruzalski, Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych w Centrum e-Zdrowia
20. Andrzej Sarnowski, Dyrektor Pionu Rozwoju SIM i Wdrożeń w Centrum e-Zdrowia
21. Wojciech Demediuk, Dyrektor Departamentu e-Zdrowia w Ministerstwie Zdrowia
22. Radosław Maćkiewicz, Dyrektor Centralnego Ośrodka Informatyki

23. Paweł Bernacik, Dyrektor Departamentu Cyberbezpieczeństwa w Centralnym Ośrodku Informatyki
24. Sebastian Nowakowski, Zastępca Dyrektora Departamentu Eksploatacji Systemów w Centralnym Ośrodku Informatyki

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

25. Karolina Taczalska, Biuro Ministra w MC
26. Joanna Gójska, Biuro Ministra w MC