Warszawa, 2025-05-19

CSIRT-CeZ.564.6.2025
(IK: 178325)

Dostawcy usług IT
dla podmiotów sektora
ochrony zdrowia

Dotyczy: Pismo w sprawie wdrożenia mechanizmów logowania wieloskładnikowego (MFA)

Szanowni Państwo,

w ramach Centrum e-Zdrowia, decyzją Ministra Zdrowia, został powołany w dniu 1 grudnia 2023 r. Sektorowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT CeZ). Funkcjonowanie sektorowych CSIRT reguluje Ustawa z dn. 1 sierpnia 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, szczególnie art. 44, definiujący poniższy zakres zadań:

1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13;
3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu;
4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Realizacja powyższego zakresu działań ustawowych pozwala na wyciągnięcie jednoznacznych wniosków, związanych z zapewnieniem bezpieczeństwa danych medycznych, spośród których fundamentalne znaczenie ma wdrożenie logowania wieloskładnikowego (MFA).

Liczba cyberataków systematycznie wzrasta. Zapewnienie bezpieczeństwa danych obywateli, szczególnie danych wrażliwych oraz zapewnienie ciągłości funkcjonowania usług w sektorze ochrony zdrowia ma charakter strategiczny dla prawidłowego funkcjonowania państwa. Newralgicznym punktem jest bezpieczeństwo kont użytkowników. Według danych Microsoft, **MFA jest w stanie zablokować nawet do 99,9% ataków** na konta użytkowników[1]. Wartość ta pozwala na wyciągniecie wniosku o wysokiej skuteczności tego rozwiązania, będącego obecnie standardem w innych sektorach strategicznych. W sektorze finansowym wykorzystanie MFA jest wręcz konieczne i wynika z przepisów Rozporządzenia Digital Operational Resilience Act (DORA).

[1] https://learn.microsoft.com/en-us/partner-center/security/security-at-your-organization, dostęp 12.05.2025 r.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Spośród wielu zalet wynikających z wdrożenia MFA najważniejsze to:

- **Ochrona dostępu do systemów i danych:**
  Nawet jeśli hasło pracownika zostanie przechwycone, atakujący nie uzyska dostępu bez dodatkowego składnika uwierzytelnienia. MFA dodaje warstwę zabezpieczeń, która skutecznie chroni przed nieautoryzowanym dostępem.

- **Zabezpieczenie przed phishingiem**:
  MFA niweluje skutki prób oszustwa polegających na wyłudzaniu haseł. Nawet jeśli użytkownik poda swoje dane logowania na fałszywej stronie, brak drugiego składnika uwierzytelnienia uniemożliwia atakującemu przejęcie konta.

Mając na uwadze powyższe, zwracamy się do Państwa z prośbą o aktywne kontynuowanie działań na rzecz podnoszeniu bezpieczeństwa przetwarzanych poprzez Państwa systemy danych. Jako CSIRT CeZ dostrzegamy coraz większą liczbę ataków skutkujących wykradzeniem danych personelu medycznego oraz fałszowaniem dokumentacji medycznej, np. nielegalnym wystawianiem recept. Zdajemy sobie sprawę, że nałożenie dodatkowych warstw cyberbezpieczeństwa może wpływać na ergonomię użytkowania systemów IT, niemniej w dobie rosnącej liczby zagrożeń w świecie cyfrowym, wdrożenie logowania wieloskładnikowego (MFA) staje się koniecznością. Celem mitygacji ryzyka związanego z niechęcią klientów i ich użytkowników do wprowadzenia obowiązkowego MFA jest bieżące informowanie o zagrożeniach oraz uświadomienie o fundamentalnej roli logowania wieloskładnikowego w procesie budowy cyberbezpieczeństwa organizacji. CSIRT CeZ będzie kontynuować działania edukacyjne związane z cyberbezpieczeństwem w sektorze ochrony zdrowia oraz zwracać uwagę na konieczność poprawy poziomu cyberhigieny, jak również wdrażanie nowych rozwiązań technologicznych, poprawiających bezpieczeństwo danych i systemów teleinformatycznych, takich jak MFA.

Podsumowując, zachęcamy Państwa do:

- cyklicznego przypominania Państwa klientom o potrzebie stosowania MFA;

- o zaletach stosowania MFA oraz ryzykach związanych z brakiem MFA;

- dążenia do wdrożenia, podobnie jak w bankach, obowiązkowego MFA.

CSIRT CeZ zapewni wsparcie w postaci udostępniania artykułów, zaleceń oraz materiałów edukacyjnych, które będziecie Państwo mogli wykorzystać jako punkt odniesienia, w kontekście wprowadzanych rozwiązań dotyczących bezpieczeństwa.

W razie pytań lub chęci zacieśnienia współpracy zachęcamy do kontaktu z Zespołem CSIRT CeZ, e-mail: info@csirt.cez.gov.pl lub kontakt z Kierownikiem Wydziału CSIRT, Panem Jeremim Olechnowiczem: j.olechnowicz@cez.gov.pl. Prosimy o przekazanie niniejszego pisma do wszystkich podmiotów zrzeszonych w Państwa organizacji.

Z poważaniem

Jeruzalski Tomasz

Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

/dokument podpisany elektronicznie/

Otrzymują:

1. Pan Bartłomiej Chudawski, Prezes Stowarzyszenia Twórców Oprogramowania Rynku Medycznego.
2. Pan Rafał Dunal, Prezes Polskiej Izby Informatyki Medycznej.

Do wiadomości:

- Pan Wojciech Demediuk, Dyrektor Departamentu e-Zdrowia, Ministerstwo Zdrowia.

Osoba sporządzająca: Kuczyński Grzegorz

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706