



# Minister Edukacji i Nauki

Przemysław Czarnek

CTC-CTC.4061.69.2023.AS  
Warszawa, 07 czerwca 2023 r.

Pan  
Marcin Wiącek  
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

odpowiadając na pismo nr VII.501.72.2023.MK z 5 maja br., w sprawie wprowadzonego w szkołach objętych Ogólnopolską Siecią Edukacyjną (OSE) systemu monitorowania zachowań w sieci B3, poniżej przedstawiam stosowne informacje i wyjaśnienia.

Przedmiotowy system powstał w ramach projektu Ogólnopolskiej Sieci Edukacyjnej, która funkcjonuje na podstawie ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz.U. z 2022 r. poz. 2454 z późn.zm.). Zgodnie z art. 5 pkt 3 ww. ustawy, do zadań operatora OSE należy świadczenie szkole usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz przeciwdziałanie dostępowi do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju uczniów.

Zarówno przygotowywany system B3 jak i wszystkie inne komponenty bezpieczeństwa sieci OSE są zgodne z założeniami przyjętymi przy tworzeniu programu OSE. Jego charakterystyka została opisana w Studium Wykonalności „Budowa węzłów bezpieczeństwa szkolnego ruchu internetowego Ogólnopolskiej Sieci Edukacyjnej” realizowanego w ramach osi priorytetowej I „Powszechny dostęp do szybkiego Internetu” Programu Operacyjnego Polska Cyfrowa na lata 2014–2020”, dalej: OSE B.

Informacja, dotycząca zamówienia publicznego, związanego z dostawą systemu monitorowania zachowań (B3) w ramach projektu OSE, była opublikowana m.in. na stronach Biuletynu Informacji Publicznej NASK-PIB.

Założeniem systemu B3 jest monitorowanie zachowania użytkowników w sieci, reakcja na mowę nienawiści, mobbing, uwodzenie itp. ochrona stacji końcowych, w tym urządzeń mobilnych. Rezultatem ma być zapewnienie bezpiecznego korzystania z internetu, w tym ochrona dzieci przed szkodliwymi treściami w internecie, wynikająca z zapisów i rekomendacji wskazanych w Europejskiej Strategii dla Lepszego internetu dla Dzieci: European Strategy for a Better Internet for Kids, z 2012 r. Strategia ta ustanawiała 5 głównych filarów działań Komisji Europejskiej, Krajów Członkowskich oraz Przedsiębiorstw w zakresie bezpieczeństwa w sieci, wśród których zawarty został priorytet dotyczący tworzenia bezpiecznego środowiska online oraz stosowania rozwiązań kontroli rodzicielskiej. Cele te są kontynuowane w ramach zaktualizowanej strategii na rzecz lepszego internetu dla dzieci (tzw. BIK+), dla której polski rząd wyraził pozytywną opinię w 2022 r.

Udział w projekcie OSE, którego elementem jest system B3, jest dla szkół dobrowolny. Jednym z założeń przy tworzeniu systemu OSE było zapewnienie szkołom narzędzi, które pozwolą na zrealizowanie zapisów art. 27 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2023 r. poz. 900 z późn. zm.), zgodnie z którym szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające. Organy prowadzące, które nie chcą korzystać z usług OSE, zgodnie z ustawą o OSE, muszą zapewnić szkołom szerokopasmowy internet i odpowiedni poziom bezpieczeństwa sieci we własnym zakresie.

Zgodnie z informacjami przekazanymi przez ministra właściwego do spraw informatyzacji, podstawą założeń systemów bezpieczeństwa OSE, w tym systemu B3, od początku ich projektowania jest zgodność z przepisami prawa oraz ochrona prywatności i danych osobowych wszystkich użytkowników. Podstawową zasadą działania systemu jest monitorowanie ruchu sieci internetowej bez ingerencji w przesyłane treści oraz prywatność użytkowników.

Aby uzyskać potwierdzenie prawidłowości przyjętych rozwiązań, założenia projektowe opisane w dokumencie Studium Wykonalności zostały zweryfikowane przez kancelię prawną w roku 2020. Opinia kancelarii, zgodnie z zapytaniem NASK – PIB, koncentrowała się wokół ochrony danych osobowych, tajemnicy korespondencji jak i tajemnicy telekomunikacyjnej wynikającej z ustawy Prawo telekomunikacyjne. Na bazie powyższej opinii zostały określone szczegółowe wymagania funkcjonalne i techniczne dla wdrażanego systemu, w tym zakres i sposób przetwarzania danych, umożliwiający działanie systemu B3 zgodnie z obowiązującymi przepisami prawa.

Operatora OSE obowiązują przepisy regulujące działalność operatorów telekomunikacyjnych świadczących usługi telekomunikacyjne na terenie RP, w tym te dotyczące konieczności ustanowienia regulaminu usług telekomunikacyjnych OSE, informowania opiekunów uczniów o fakcie rozpoczęcia działania systemu oraz zbierania i przetwarzania danych przez system w celach naukowych i badawczych. Powyższe zagadnienia były przedmiotem kolejnych analiz prawnych, zaś otrzymane opinie prawne potwierdziły zgodność z obowiązującymi przepisami prawa założeń funkcjonowania systemu B3 oraz celu, do którego został on przeznaczony.

Prace nad aspektami ochrony danych osobowych były również prowadzone na etapie przygotowywania programu OSE. W 2017 roku odbyło się spotkanie w ówczesnym Biurze GłODO, podczas którego zostały omówione szczegóły planowanych działań ze szczególnym uwzględnieniem tematu przetwarzania danych osobowych w planowanych do wdrożenia systemach bezpieczeństwa OSE. Tematami konsultacji były następujące zagadnienia:

- podstawy prawne umożliwiające wdrożenie planowanych systemów bezpieczeństwa w sieci OSE,
- ryzyka prawne mogące wystąpić w związku ze stosowaniem ww. systemów,
- neutralność sieci (rozumianej jako traktowanie ruchu na równych zasadach, niezależnie od źródła jego pochodzenia, wykorzystywanej aplikacji, miejsca docelowego, wykorzystanego protokołu lub treści komunikacji) z uwzględnieniem aspektu dopuszczalności blokowania dostępu do wybranych zasobów sieciowych,
- tajemnica korespondencji w ramach przetwarzanego przez Operatora OSE ruchu sieciowego.

Przeprowadzone konsultacje pozwoliły wybrać odpowiedni model wdrażanych systemów bezpieczeństwa OSE i usług uwzględniający wymagania ustawowe, tak aby zachować odpowiednią równowagę pomiędzy zachowaniem wymaganej prawem prywatności użytkowników OSE, a zdolnością systemów bezpieczeństwa OSE do skutecznego wykrywania zagrożeń i ich zapobieganiu.

Usługi bezpieczeństwa, zbudowane w ramach programu OSE, zostały podzielone na poziomy odpowiadające za poszczególne obszary zagrożeń. Komunikacja pomiędzy szkołami i internetem odbywa się za pośrednictwem poszczególnych systemów bezpieczeństwa, z których każdy w kolejnych krokach dokonuje analizy przesyłanych treści. Należy podkreślić, iż jedynie wybrane rodzaje komunikacji są poddawane przedmiotowej analizie, na końcu której znajduje się system B3. Złożona architektura systemów bezpieczeństwa pomija analizę ruchu w przypadku komunikacji dotyczącej wiadomości poczty elektronicznej, komunikatorów internetowych, jak również wszystkich portali internetowych,

które mogą zawierać dane wrażliwe bądź umożliwiające identyfikację użytkownika, w szczególności takich jak systemy transakcyjne banków, portale urzędowe czy służby zdrowia. Co ważne, system B3 w pierwszym kroku swojego działania, na dopuszczonych rodzajach komunikacji, dokonuje jednokierunkowej, nieodwracalnej anonimizacji danych, dzięki czemu nie jest możliwe ich ponowne odtworzenie. Dzięki realizacji powyższych założeń projektowych, system B3 nie ingeruje w życie prywatne uczniów i nauczycieli, dotyka jedynie tych treści, które nie zawierają co do zasady danych wrażliwych.

Po dokonaniu przez system B3 anonimizacji danych, są one przetwarzane przez poszczególne komponenty systemu. Dane są analizowane przez poszczególne klasyfikatory, dokonujące weryfikacji treści (tekst, obraz i video) i wskazujące na występowanie treści o charakterze potencjalnie szkodliwym. Zagregowane dane o dostępie do treści potencjalnie szkodliwych będą podstawą do przygotowania raportu dla dyrektora szkoły. Raport będzie zawierał informacje statystyczne dotyczące poszczególnych kategorii w odniesieniu do danej szkoły. Raporty dla dyrektora szkoły, tworzone w oparciu o system B3, pozwolą na planowanie celowanych działań w zakresie poszczególnych kategorii problemów zaobserwowanych w danej szkole.

Z informacji przekazanych przez ministra właściwego do spraw informatyzacji wynika również, że zgodnie z obecnym harmonogramem wdrożenia i uruchomienia systemu B3 oraz udostępnienia usługi bezpieczeństwa świadczonej w oparciu o ten system do korzystania przez dyrektorów szkół, jest on obecnie w fazie „uczenia” (zgodnie z mechanizmami działania AI - sztucznej inteligencji). Zastosowane w systemie mechanizmy klasyfikacji danych opierają się, oprócz narzędzi słownikowych, na narzędziach sztucznej inteligencji, przede wszystkim na uczeniu maszynowym.

Mechanizmy te wymagają precyzyjnego dostrojenia tak, aby efektem ich działania były prawidłowe informacje przekazywane dyrektorom szkół, nieobarczone błędami wynikającymi z nieprawidłowej klasyfikacji danych. Obecna faza kalibracji (douczania) systemu B3 jest konieczna i była planowana w założeniach dotyczących terminu udostępnienia dyrektorom szkół kolejnej usługi z zakresu bezpieczeństwa teleinformatycznego. W ramach uczenia systemu budowana jest baza wiedzy o charakterze i specyfice ruchu przetwarzanego w szkołach. Tworzenie optymalnego modelu ruchu jest niezbędne do precyzyjnego wskazywania, które treści są faktycznie potencjalnie szkodliwe. Działanie to ma na celu minimalizację błędów w przyszłych raportach.

Mając to na uwadze, w ocenie Ministerstwa Edukacji i Nauki, udostępnianie dyrektorom szkół raportów na etapie uczenia się systemu należy uznać za przedwczesne.

W trakcie procesu „uczenia” systemu B3, związanego z analizą wyników działania tego systemu, system B3 wykonuje obecnie bardzo ważne zadanie – poprawia jakość blokowania potencjalnie szkodliwych treści w innych systemach bezpieczeństwa OSE. Na podstawie analizy ruchu, system B3 odnajduje, na przykład na podstronach portali, materiały nieodpowiednie dla najmłodszych użytkowników sieci i oznacza je jako potencjalnie szkodliwe. Informacja ta, przekazywana do innych systemów bezpieczeństwa OSE, stanowi podstawę do uzupełnienia ich baz reputacyjnych. W efekcie działania systemu B3 i jego wpływu na konfigurację systemów bezpieczeństwa OSE, rozpoznanie jednej treści potencjalnie szkodliwej w jednej tylko szkole, daje możliwość zablokowania jej dla wszystkich szkół w Polsce na innych poziomach bezpieczeństwa OSE. W ten sposób każdego dnia będzie zwiększane bezpieczeństwo uczniów.

Realizowany obecnie harmonogram działań zakłada udostępnienie szkołom wyników pracy systemu B3 przez portal Moje OSE na początku roku szkolnego 2023 / 2024.

Ministerstwo Edukacji i Nauki będzie uważnie monitorowało funkcjonowanie systemu po zakończeniu jego uczenia się i analizowało przydatność raportów dla prawidłowego funkcjonowania szkół. W mojej ocenie raporty udostępniane dyrektorom szkół mogą przyczynić się do podejmowania przez nich właściwych decyzji zarówno w sprawach doraźnych, jak i podczas planowania działań w dłuższej perspektywie czasowej – np. w ramach programów wychowawczo – profilaktycznych.

Z wyrazami szacunku

Przemysław Czarnek  
Minister  
/ – podpisano cyfrowo/