NASK

Warszawa, 19 maja 2023 r.

ZBPOSE.072.1.2023

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Biuro Rzecznika Praw Obywatelskich
al. Solidarności 77
00-090 Warszawa

Szanowny Panie Rzeczniku,

w odpowiedzi na pismo z dnia 5 maja 2023 r. (znak: VII.501.72.2023.MK) dot. systemu monitorowania zachowań w sieci (tzw. system B3) wprowadzonego w szkołach objętych Ogólnopolską Siecią Edukacyjną (OSE) przedstawiamy poniżej aktualny status i odpowiedzi na pytania zawarte w piśmie.

Odpowiadając na pytanie dotyczące podstaw prawnych działania systemu, należy odwołać się przede wszystkim do Ustawy o Ogólnopolskiej Sieci Edukacyjnej z dnia 27 października 2017 roku. 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.

Zarówno przygotowywany system B3 jak i wszystkie inne komponenty bezpieczeństwa budujące ekosystem bezpieczeństwa sieci OSE są zgodne z założeniami przyjętymi przy tworzeniu programu OSE. Jego charakterystyka została opisana w Studium Wykonalności projektu „**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.

NASK-PIB
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

BNP Paribas Bank Polska Spółka Akcyjna
z siedzibą w Warszawie
ul. Kasprzaka 2, 01-211 Warszawa
Numer konta:
28 1750 0009 0000 0000 0094 9997

www.nask.pl

NASK

Podstawą założeń systemów bezpieczeństwa OSE, w tym systemu B3, od początku ich projektowania jest absolutna zgodność z przepisami prawa, 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 kancelarię 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 GIODO, na którym zostały omówione szczegóły planowanych działań ze szczególnym uwzględnieniem tematu przetwarzania danych osobowych w planowanych do wdrożenia systemach bezpieczeństwa OSE. Tematami konsultacji były 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.

Ekosystem bezpieczeństwa zbudowany w ramach programu OSE, został podzielony 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. Kluczowy jest fakt, 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.

Usługi bezpieczeństwa OSE mają charakter dobrowolny, a to oznacza, iż dyrektor szkoły decyduje, czy równocześnie z korzystaniem z usług dostępu do internetu OSE, korzysta z usług bezpieczeństwa dostarczanych przez OSE, czy też zapewnia ochronę przed treściami szkodliwymi w internecie we własnym zakresie. Usługi bezpieczeństwa w ramach projektu OSE, które są obecnie udostępnione do korzystania przez szkoły, zawierają szereg elementów ochrony przed

cyberzagrożeniami. Usługi te zapewniają kompleksową ochronę przed zagrożeniami, pracując w różnych obszarach technologicznych. Ochrona przed szkodliwymi treściami jest realizowana na bazie systemu bezpiecznego DNS, który wykorzystuje bazę reputacyjną zawierającą domeny rozpoznane jako szkodliwe w poszczególnych kategoriach treści i blokuje dostęp do nich – ten poziom bezpieczeństwa nazywany jest B1. Analogicznie działa system Security Web Gateway (system B2), który w oparciu o własne bazy reputacyjne dokonuje klasyfikacji poszczególnych adresów URL i zapewnia blokowanie dostępu do nich. Warto podkreślić, jak wspomniano powyżej, że system B3 nie będzie pełnił takiej roli jak wspomniane powyżej systemy, nie będzie wprowadzał bezpośredniej blokady dostępu do treści. System B3 będzie taki ruch monitorował i przekazywał raporty o próbach dostępu do treści potencjalnie szkodliwych dyrektorowi szkoły.

W zakresie aspektów technicznych systemu B3, jak wspomniano powyżej, system na wstępie analizy ruchu dokonuje anonimizacji danych, które są następnie 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. Już dziś jednak, różnorodne materiały edukacyjne (kursy e-learningowe, scenariusze lekcji, poradniki) z zakresu bezpiecznego korzystania z sieci internet są dostępne na platformie OSE IT Szkoła (it-szkola.edu.pl). Mogą z nich bezpłatnie korzystać nauczyciele, dyrektorzy, a także rodzice i sami uczniowie. NASK – PIB regularnie zachęca do tego w ramach działań edukacyjno-informacyjnych realizowanych w ramach programu OSE.

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

NASK

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.

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 zwiększane jest bezpieczeństwo uczniów.

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

Z poważaniem,
p.o. Dyrektora Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego
Wojciech Pawlak

NASK-PIB
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

BNP Paribas Bank Polska Spółka Akcyjna
z siedzibą w Warszawie
ul. Kasprzaka 2, 01-211 Warszawa
Numer konta:
28 1750 0009 0000 0000 0094 9997

www.nask.pl